

Monthly Security Bulletin

This security bulletin is powered by Telelink's Advanced Security Operations Center

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

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

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



Why Advanced Security Operations Center (ASOC) by Telelink?

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

LITE Plan

425 EUR/mo

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

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

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

Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

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

Complete visibility, deep analysis and cyber threat mitigation!

TELELINK PUBLIC

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.	Securing Space 4.0 – One Small Step or a Giant Leap? Part 2	4
2.	Fake Investor John Bernard Walked Away With \$30M	13
3.	Autonomous Vehicle Security Needs From A Hacker's Perspective	17
4.	Software AG IT giant hit with \$23 million ransom by Clop ransomware	19
5.	Microsoft Uses Trademark Law to Disrupt Trickbot Botnet	23
6.	Windows Update can be abused to execute malicious programs.....	27
7.	Nation-state actor hit Google with the largest DDoS attack.....	30
8.	Watch out for Emotet malware's new 'Windows Update' attachment	32
9.	Rapper Scams \$1.2M in COVID-19 Relief, Gloats with 'EDD' Video.....	35
10.	French IT giant Sopra Steria hit by Ryuk ransomware	37
11.	The Importance of Good Cyber Hygiene — Now More than Ever	39
12.	Google employees personal info exposed in law firm data breach	43
13.	Enel Group hit by ransomware again, Netwalker demands \$14 million	44
14.	Maze ransomware is shutting down its cybercrime operation.....	48

1. Securing Space 4.0 – One Small Step or a Giant Leap? Part 2

McAfee Advanced Threat Research (ATR) is collaborating with [Cork Institute of Technology \(CIT\)](#) and its [Blackrock Castle Observatory \(BCO\)](#) and the [National Space Center](#) in Cork, Ireland

In the [first of this two-part blog series](#) we introduced Space 4.0, its data value and how it looks set to become the next battleground in the defense against cybercriminals. In part two we discuss the architectural components of Space 4.0 to threat model the ecosystem from a cybersecurity perspective and understand what we must do to secure Space 4.0 moving forward.

Nanosats: Remote Computers in Space

A satellite is composed of a [payload and a bus](#). The payload is the hardware and software required for the mission or satellite's specific function, such as imaging equipment for surveillance. The bus consists of the infrastructure or platform that houses the payload, such as thermal regulation and command and control. [Small satellites](#) are space craft typically weighing less than 180 kilograms and, within that class of satellites, is what we call nanosatellites or nanosats which typically weigh between 1-10 kilograms. Cubesats are a class of nanosat so you will often hear the term used interchangeably, and for the context of Space 4.0 security, we can assume they are the same device. Nanosats significantly reduce launch costs due to their small size and the fact that many of these devices can be mounted on board a larger single satellite for launch.

[Commercial off-the-shelf](#) (COTS) Cubesats typically use free open source software such as FreeRTOS or KubOS for the on-board operating system. However, other systems are possible, with drivers available for most of the hardware on Linux and Windows OS. [KubOS](#) is an open source flight software framework for satellites and has cloud-based mission control software, [Major Tom](#), to operate nanosats or a constellation. We mention KubOS here as it is a good example of what the current Space 4.0 operating model looks like today. While we have not reviewed KubOS from a security perspective, developing a secure framework for satellites is the right path forward, allowing mission developers to focus on the payload.

Some of the use cases available with Cubesats are:

- File transfers
- Remote communication via uplink/downlink
- Intra-satellite and inter-satellite communications
- Payload services such as camera and sensors telemetry
- Software Updates

KubOS is “[creating a world where you can operate your small satellite from your web browser or iPhone](#)”. [KubOS’ objective](#) is to allow customers to send bits and not rockets to space and it is defining a new era of software-designed satellites. The satellite model is changing from relay type devices to remote computers in space using COTS components and leveraging TCP/IP routing capabilities. This model shift also means that there is more software executing on these satellites and more complex payload processing or interaction with the software stack and hence more attack surface.

To date, attacks on satellite systems from a cybersecurity perspective have typically been in the context of VSAT terminals, eavesdropping and hijacking. While there have been vulnerabilities found in the VSAT terminal software and its higher-level custom protocols, there seems to have been no focus and vulnerabilities discovered within the network software stack of the satellite itself. This may be since satellites are very expensive, as well as closed source, so not accessible to security researchers or cybercriminals, but this security by obscurity will not provide protection with the new era of nanosats. Nanosats use COTS components which will be accessible to cybercriminals.

Due to the closed nature of satellites there has not been much published on their system hardware and software stack. However, the [Consultative Committee for Space Data Systems \(CCSDS\)](#), which develops standards and specifications including protocols for satellite communications, does give some insight. The [CCSDS technical domains](#) are:

- Space Internetworking Services
- Mission Ops. And Information Management Services
- Spacecraft Onboard Interface Services
- System Engineering
- Cross Support Services
- Space Link Services

The CCSDS standards are divided into color codes to represent recommended standards and practices versus informational and experimental. This is a very large source of data communications for satellite designers to aid them in a reference for implementation. However, as we have observed over the cyber threat landscape of the past few decades, secure standards and specifications for hardware, software and protocols do not always translate to secure implementation. The CCSDS defines a TCP/IP stack suitable for transmission over space datalinks as per figure 1 below. Satellites that become more connected, just like any other device on the internet, their network and protocol software stack will become more accessible and targeted. As we discussed in part 1 <insert link> of our Space 4.0 blog series, there have been many TCP/IP and remote protocol related vulnerabilities in both embedded devices and even state of the art operating systems such as Windows 10. The TCP/IP stack and remote protocol implementations are a common source of vulnerabilities due to the complexities of parsing in unsafe memory languages such as C and C++. There does not appear to be any open source implementations of the CCSDS TCP/IP protocol stack.

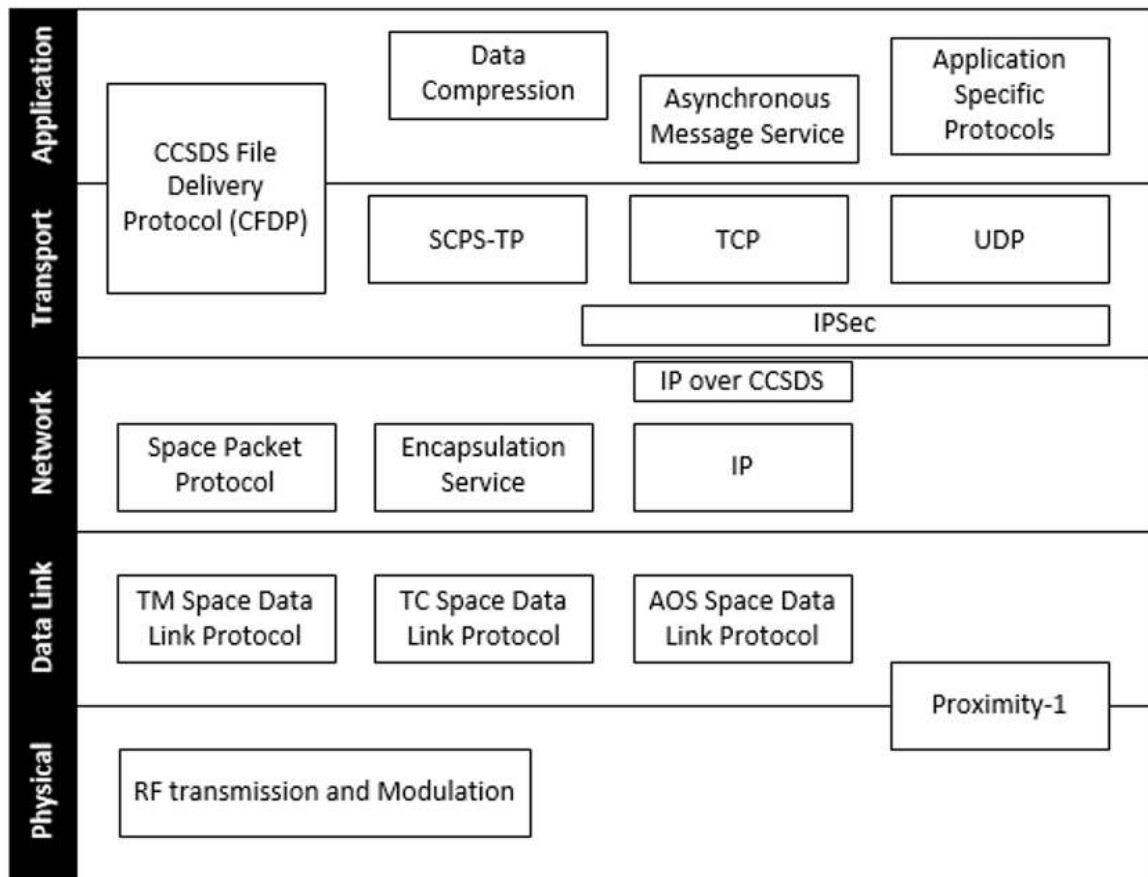


Figure 1 – CCSDS [Space communications protocols reference model](#)

The [CubeSat Protocol](#) (CSP) is a free open source TCP/IP stack implementation for communication over space datalinks, similar to the CCSDS TCP/IP stack. The [CSP protocol library](#) is implemented in C, open source and implemented in many Cubesats that have been deployed to space. The protocol can be used for communication from ground station to satellite, inter-satellite and the intra-satellite communication bus. There have been [3 vulnerabilities](#) to date reported in this protocol.

Figure 2 below shows what a Cubesat architecture looks like from a trust boundary perspective relative to the satellite and other satellites within the constellation and the earth.

Figure 2 – Space LEO Cubesat architecture trust boundaries

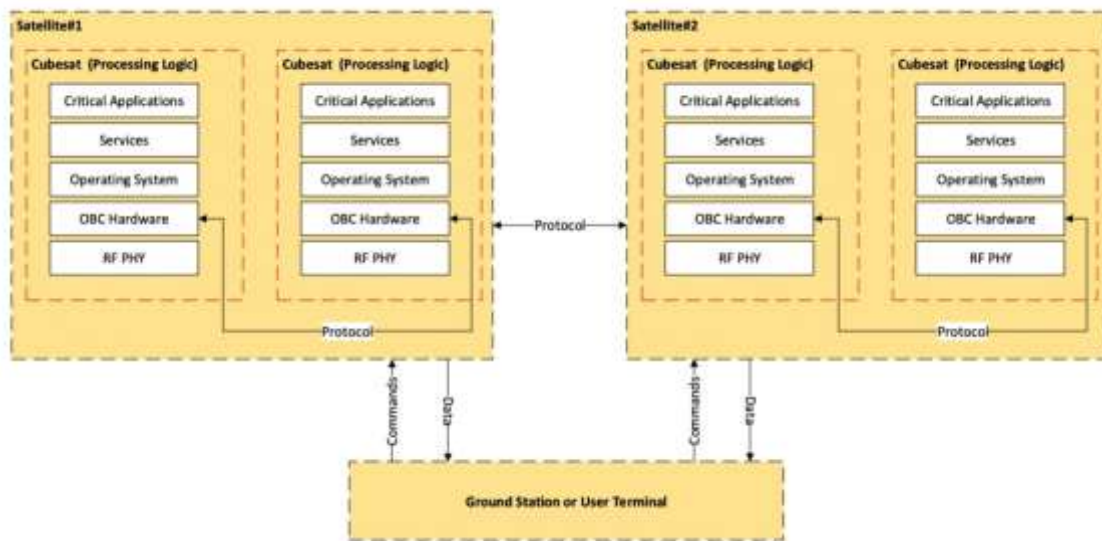


Figure 2 – Space LEO Cubesat architecture trust boundaries

No hardware, software, operating system or protocol is completely free of vulnerabilities. What is important from a security perspective is:

- The accessibility of the attack surface
- The motives and capabilities of the adversary to exploit an exposed vulnerability if present in the attack surface

As these low-cost satellites get launched in our LEO and become more connected, any exposed technology stack will become increasingly targeted by cybercriminals.

Space 4.0 Threat Modeling

This Space 4.0 threat model focuses on the cybercriminal and how they can exploit Space 4.0 data for monetization. The [following Space 4.0 factors](#) will make it more accessible to cybercriminals:

- Mass deployment of small satellites to LEO
- Cheaper satellites with COTS components and increased satellite on board software processing (no longer relay devices)
- Satellite service models, Ground Station-as-a-Service (GSaaS) and Satellite-as-a-Service (SataaS) and shared infrastructure across government, commercial and academic
- Satellite connectivity and networks in space (ISL – inter-satellite links)
- Space 4.0 data value

[Space security has typically been analyzed](#) from the perspective of ground segment, communications or datalink and space segment. Additionally, the attack classes have been categorized as electronic (jamming), eavesdropping, hijacking and control. Per figure 3

below, we need to think about Space 4.0 with a cybersecurity approach due to the increased connectivity and data, as opposed to the traditional approach of ground, communication and space segments. Cybercriminals will target the data and systems as opposed to the RF transmission layer.

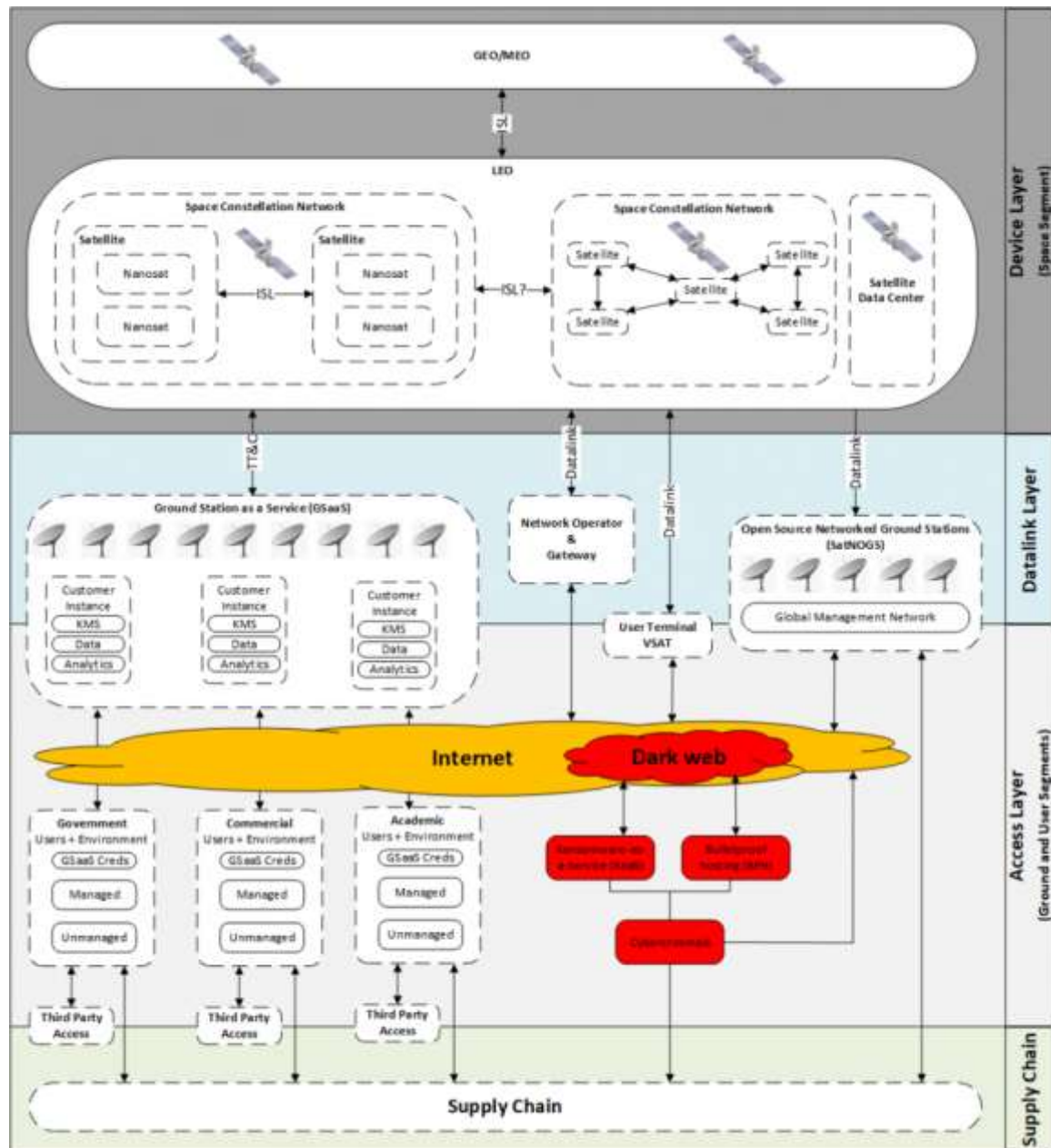


Figure 3 – Space 4.0 threat modeling architecture

It is important to consider the whole interconnectivity of the Space 4.0 ecosystem as cybercriminals will exploit any means possible, whether that be direct or indirect access (another trusted component). Open source networked ground stations such as [SatNOGS](#) and the emerging [NyanSat](#) are great initiatives for space research but we should consider these in our overall threat model as they provide mass connectivity to the internet and space.

The traditional space security model has been built on a foundation of cost as a barrier to entry and perimeter-based security due to lack of physical access and limited remote access to satellites. However, once a device is connected to the internet the threat model changes and we need to think about a satellite as any other device which can be accessed either directly or indirectly over the internet.

In addition, if a device can be compromised in space remotely or through the supply chain, then that opens a new attack class of space to cloud/ground attacks.

Users and trusted insiders will always remain a big threat from a ground station perspective, just like enterprise security today, as they can potentially get direct access to the satellite control.

The movement of ground services to the cloud is a good business model if designed and implemented securely, however a compromise would impact many devices in space being controlled from the GSaaS. It is not quite clear where the shared responsibility starts and ends for the new SaaS and GSaaS Space 4.0 service models but the satellite key management system (KMS), data, GSaaS credentials and analytics intellectual property (this may reside in the user's environment, the cloud or potentially the satellite but for the purposes of this threat model we assume the cloud) will be much valued assets and targeted.

From the Cyber and Space Threat Landscape review in part 1 [<insert link>](#), combined with our understanding of the Space 4.0 architecture and attack surfaces, we can start to model the threats in Table 1 below.

Threats	Attack Classes	Attack Vectors
<ul style="list-style-type: none"> • Data theft • Ransomware • Analytics IP theft • Satellite Control • Mass satellite DDoS from networked ground stations • Bulletproof hosting (BPH) • Critical infrastructure or mission disruption • Satellite collision • Satellite take over • Cloud GSaaS take over • Malware and Ransomware distribution via Open Source Ground Stations • Compromised Nanosat communications for Botnet • Malware and Ransomware distribution via nanosats (constellation worms) 	Data (Device, Datalink and Access layers)	Nanosat downlink interception
		Space storage data center interfaces
		Insecure cloud data storage service APIs
		Exploit gaps in shared security model
	Supply Chain	Open source hardware and software backdoors
		Third party compromise and transient trust
	Cloud Service Provider (CSP) Ground Station (Access layer)	GSaaS or SaaS credential compromise via phishing
		Cloud misconfigurations and infrastructure
		Identity and access management compromise
		Insecure GSaaS and SaaS service model APIs
		Trusted insider
	Cloud to Space (Access and Datalink layers)	Compromise of GSaaS credentials
		Protocol software vulnerabilities
		Nanosat uplink control
		Supply chain attack on space data center
	Space to Cloud (Device and Datalink layers)	Network operator gateway protocol software attacks
		Compromised satellite device due to supply chain attack
	Constellation (Device layer)	Remote protocol software vulnerabilities
		Intra-Satellite due to protocol software vulnerability allowing satellite payload to interact with satellite bus
		Inter-Satellite link (ISL) due to protocol software vulnerability
		Inter-Constellation ISL due to protocol software vulnerability (unclear right now if this use case will be possible in the future)
		Supply chain attack
		Protocol software vulnerability on space data center satellite

Table 1 – Space 4.0 threats, attack classes and layers, and attack vectors

Based on the above threat model, let's discuss a real credible threat and attack scenario. From our Space cyber threat landscape review in part 1 of this blog series, there were

attacks on ground stations in 2008 at the Johnson Space Center and for a Nasa research satellite. In a Space 4.0 scenario, the cybercriminal attacks the ground station through phishing to get access to satellite communications (could also be a supply chain attack to get a known vulnerable satellite system into space). The cybercriminal uses an exploit being sold on the underground to exploit a remote wormable vulnerability within the space TCP/IP stack or operating system of the satellite in space, just like we saw EternalBlue being weaponized by WannaCry. Once the satellite has been compromised the malware can spread between satellite vendors using their ISL communication protocol to propagate throughout the constellation. Once the constellation has been compromised the satellite vendor can be held to ransom, causing major disruption to Space 4.0 data and/or critical infrastructure.

Moving Forward Securely for a Trustworthy Space 4.0 Ecosystem

Establishing a trustworthy Space 4.0 ecosystem is going to require strong collaboration between cyber threat research teams, government, commercial and academia in the following areas:

- [Governance and regulation](#) of security standards implementation and certification/validation of satellite device security capabilities prior to launch
- Modeling the evolving threat landscape against the Space 4.0 technology advancements
- Secure reference architectures for end to end Space 4.0 ecosystem and data protection
- Security analysis of the CCSDS protocols
- Design of trustworthy platform primitives to thwart current and future threats must start with a security capable bill of materials (BOM) for both hardware and software starting with the processor then the operating system, frameworks, libraries and languages. Hardware enabled security to achieve confidentiality, integrity, availability and identity so that satellite devices may be resilient when under attack
- Visibility, detection and response capabilities within each layer defined in our Space 4.0 architecture threat model above
- Development of a MITRE ATT&CK specifically for Space 4.0 as we observe real world incidents so that it can be used to strengthen the overall defensive security architecture using TTPs and threat emulation

Space 4.0 is moving very fast with GSaaS, SataaS and talk of space data centers and high-speed laser ISL; security should not be an inhibitor for time to market but a contributor to ensure that we have a strong security foundation to innovate and build future technology

on with respect to the evolving threat landscape. Space communication predates the Internet so we must make sure any legacy limitations which would restrict this secure foundation are addressed. As software complexity for on board processing and connectivity/routing capability increases by moving to the edge (space device) we will see vulnerabilities within the Space 4.0 TCP/IP stack implementation.

This is a pivotal time for the secure advancement of Space 4.0 and we must learn from the mistakes of the past with IoT where the rush to adopt new and faster technology resulted in large scale deployment of insecure hardware and software. It has taken much effort and collaboration between Microsoft and the security research community since [Bill Gates announced the Trustworthy Computing initiative](#) in 2002 to arrive at the state-of-the-art Windows 10 OS with hardware enabled security. Likewise, we have seen great advancements on the IoT side with [ARM Platform Security Architecture](#) and [Azure Sphere](#). Many security working groups and bodies have evolved since 2002, such as [the Trust Computing Group](#), [Confidential Computing Consortium](#), [Trusted Connectivity Alliance](#) and [Zero Trust](#) concept to name a few. There are many trustworthy building block primitives today to help secure Space 4.0, but we must leverage at the concept phase of innovation and not once a device has been launched into space; the time is now to secure our next generation infrastructure and data source. Space security has not been a priority for governments to date but that seems all set to change with the "[Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems](#)".

We should pause here for a moment and recognize the recent efforts from the cybersecurity community to secure space, such as the [Orbital Security Alliance](#), [S-ISAC](#), [Mantech](#) and Defcon [Hack-a-Sat](#).

[KubOS is being branded](#) as the Android of space systems and we are likely to see a myriad of new software and hardware emerge for Space 4.0. We must work together to ensure Space 4.0 connectivity does not open our global connectivity and infrastructure dependency to the next Mirai botnet or WannaCry worm on LEO.

McAfee would like to thank [Cork Institute of Technology](#) (CIT) and its [Blackrock Castle Observatory](#) (BCO) and the [National Space Center](#) (NSC) in Cork, Ireland for their collaboration in our mission to secure Space 4.0.

The post [Securing Space 4.0 – One Small Step or a Giant Leap? Part 2](#) appeared first on [McAfee Blogs](#).

Source: <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/securing-space-4-0-one-small-step-or-a-giant-leap-part-2/>

2. Fake Investor John Bernard Walked Away With \$30M

September featured [two stories](#) on a phony tech investor named **John Bernard**, a pseudonym used by a convicted thief named **John Clifton Davies** who's fleeced dozens of technology companies out of an estimated \$30 million with the promise of lucrative investments. Those stories prompted a flood of tips from Davies' victims that paints a much clearer picture of this serial con man and his cohorts, including allegations of hacking, smuggling, bank fraud and murder.

KrebsOnSecurity interviewed more than a dozen of Davies' victims over the past five years, none of whom wished to be quoted here out of fear of reprisals from a man they say runs with mercenaries and has connections to organized crime.

As described in [Part II of this series](#), John Bernard is in fact John Clifton Davies, a 59-year-old U.K. citizen who absconded from justice before being convicted on multiple counts of fraud in 2015. Prior to his conviction, Davies served 16 months in jail before being cleared of murdering his third wife on their honeymoon in India.



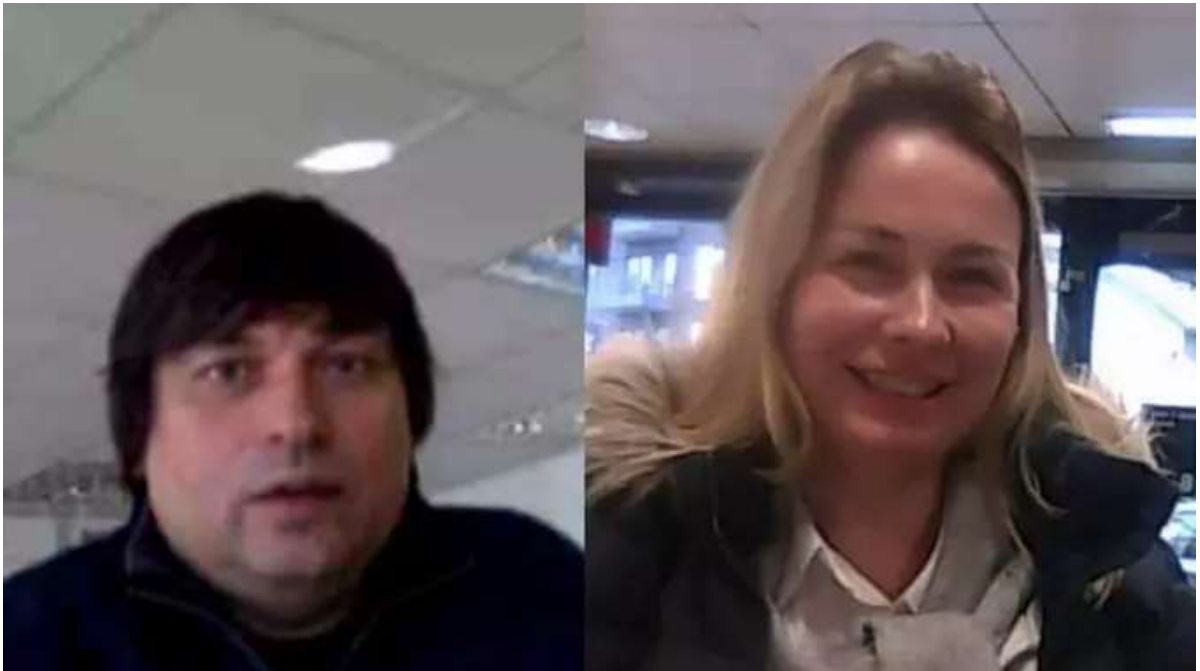
The scam artist John Bernard (left) in a recent Zoom call, and a photo of John Clifton Davies from 2015.

After eluding justice in the U.K., Davies reinvented himself as [The Private Office of John Bernard](#), pretending to be a billionaire Swiss investor who made his fortunes in the dot-com boom 20 years ago and who was seeking investment opportunities. In case after case, Bernard would promise to invest millions in tech startups, and then insist that companies pay tens of thousands of dollars worth of due diligence fees up front. However, the due diligence company he insisted on using — another Swiss firm called [Inside Knowledge](#) — also was secretly owned by Bernard, who would invariably pull out of the deal after receiving the due diligence money.

Bernard found a constant stream of new marks by offering extraordinarily generous finders fees to investment brokers who could introduce him to companies seeking an infusion of cash. When it came time for companies to sign legal documents, Bernard's victims interacted with a 40-something Inside Knowledge employee named "**Katherine Miller**," who claimed to be his lawyer.

It turns out that Katherine Miller is a onetime Moldovan attorney who was previously known as **Ecaterina "[Katya](#)" Dudorenko**. She is listed as a Romanian lawyer in the **U.K. Companies House** records for several companies tied to John Bernard, including [Inside Knowledge Solutions Ltd.](#), [Docklands Enterprise Ltd.](#), and [Secure Swiss Data Ltd](#) (more on Secure Swiss data in a moment).

Another of Bernard's associates listed as a director at Docklands Enterprise Ltd. is **Sergey Valentinov Pankov**. This is notable because in 2018, [Pankov and Dudorenko were convicted of cigarette smuggling in the United Kingdom](#).



Sergey Pankov and Ecaterina Dudorenko, in undated photos. Source: Mynewsdesk.com

According to the [Organized Crime and Corruption Reporting Project](#), "illicit trafficking of tobacco is a multibillion-dollar business today, fueling organized crime and corruption [and] robbing governments of needed tax money. So profitable is the trade that tobacco is the world's most widely smuggled legal substance. This booming business now stretches from counterfeiters in China and renegade factories in Russia to Indian reservations in New York and warlords in Pakistan and North Africa."

Like their erstwhile boss Mr. Davies, both Pankov and Dudorenko disappeared before their convictions in the U.K. They were sentenced in absentia to two and a half years in prison.

Incidentally, Davies was detained by Ukrainian authorities in 2018, although he is not mentioned by name in [this story](#) from the Ukrainian daily *Pravda*. The story notes that the suspect moved to Kiev in 2014 and lived in a rented apartment with his Ukrainian wife. John's fourth wife, **Iryna Davies**, is listed as a director of [one of the insolvency consulting businesses](#) in the U.K. that was part of John Davies' 2015 fraud conviction. *Pravda* reported that in order to confuse the Ukrainian police and hide from them, Mr. Davies constantly changed their place of residence.



John Clifton Davies, a.k.a. John Bernard. Image: Ukrainian National Police.

The *Pravda* story says Ukrainian authorities were working with the U.K. government to secure Davies' extradition, but he appears to have slipped away once again. That's according to one investment broker who's been tracking Davies' trail of fraud since 2015.

According to that source — who we'll call "Ben" — Inside Knowledge and The Private Office of John Bernard have fleeced dozens of companies out of nearly USD \$30 million in due diligence fees over the years, with one company reportedly paying over \$1 million.

Ben said he figured out that Bernard was Davies through a random occurrence. Ben said he'd been told by a reliable source that Bernard traveled everywhere in Kiev with several armed guards, and that his entourage rode in a convoy that escorted Davies' [high-end Bentley](#). Ben said Davies' crew was even able to stop traffic in the downtown area in what was described as a quasi military maneuver so that Davies' vehicle could proceed unobstructed (and presumably without someone following his car).

Ben said he's spoken to several victims of Bernard who saw phony invoices for payments to be made to banks in Eastern Europe appear to come from people within their own organization shortly after cutting off contact with Bernard and his team. While Ben allowed that these invoices could have come from another source, it's worth noting that by virtue of participating in the due diligence process, the companies targeted by these schemes would have already given Bernard's office detailed information about their finances, bank accounts and security processes.

In some cases, the victims had agreed to use Bernard's **Secure Swiss Data** software and services to store documents for the due diligence process. Secure Swiss Data is one of several firms [founded by Davies/Inside Knowledge](#) and [run by Dudorenko](#), and it advertised itself as a Swiss company that provides encrypted email and data storage services. In February 2020, Secure Swiss Data [was purchased in an "undisclosed multimillion buyout"](#) by **SafeSwiss Secure Communication AG**.

Shortly after [the first story on John Bernard was published here](#), virtually all of the employee profiles tied to Bernard's office removed him from their work experience as listed on their LinkedIn resumes — or else deleted their profiles altogether. Also, John Bernard's main website — [the-private-office.ch](#) — replaced the content on its homepage with a note saying it was closing up shop. Incredibly, even after the first two stories ran, Bernard/Davies and his crew continued to ply their scam with companies that had already agreed to make due diligence payments, or that had made one or all of several installment payments.

One of those firms actually issued a press release in August saying it had been promised an infusion of millions in cash from John Bernard's Private Office. They declined to be quoted here, and continue to hold onto hope that Mr. Bernard is not the crook that he plainly is.

Source: <https://krebsonsecurity.com/2020/10/promising-infusions-of-cash-fake-investor-john-bernard-walked-away-with-30m/>

3. Autonomous Vehicle Security Needs From A Hacker's Perspective

With connected cars becoming more common, the industry has more standards and options when it comes to autonomous vehicle security.

Adam Laurie, known in hacker circles as Major Malfunction, leads X-Force Red's [automotive testing practice](#). He has seen firsthand how easy it can be to compromise an autonomous vehicle if strong security processes and controls are not in place. He recently found an opening in the keyless entry device of his own vehicle, then leveraged it to unlock every vehicle of the same model in a parking lot. The project was for research purposes as opposed to a real attack, but it did show how easy it could be for an attacker to purchase a vehicle, reverse engineer it to find flaws and then exploit those flaws to compromise every other vehicle of that same model.

Laurie and IBM's Global Solution Leader for Connected Vehicle Security, Giuseppe Serio, recently presented a webinar about the regulation. They discussed the nuts and bolts of the mandate, the timeline for compliance and what automakers should be doing now to begin the compliance process.

[Watch the recording](#)

Industry Warned About Autonomous Vehicle Security

If you haven't already taken a ride inside an autonomous or semi-autonomous vehicle, chances are you will in the near future. The autonomous vehicle market is projected to [grow](#) at a compound annual growth rate (CAGR) of 68.94% from 2025 to 2030. This growth has many positives, including more lives saved.

According to the National Highway Traffic Safety Administration (NHTSA), 94% of serious crashes are due to [human error](#). As the NHTSA also points out, autonomous vehicles can cut down on traffic congestion and carbon dioxide emissions.

With the benefits comes one downside — autonomous vehicle security concerns. As with most things that connect to the internet, risks can arise, and the components of an autonomous vehicle may have inherent openings. Even if the vehicle was designed securely, new problems may surface once it is connected.

In 2019, [the FBI issued a warning](#) about autonomous vehicle cybersecurity, with "ransomware infections, data breaches leading to the exfiltration of personally identifiable information and unauthorized access to enterprise networks" likely in the future.

Dude, Where's My (Autonomous) Car?

One of the main challenges with securing autonomous vehicles is protecting its linked applications in [jailbroken phones or laptops](#), Laurie says. If an attacker were to jailbreak their own phone, they could see the application code while it was running, which includes how it talks to the backend server. They could then retrieve the application's hidden data, such as credentials, and take full control of the code, vehicle and connected infrastructure.

The vehicle itself can also be a prime target for attackers. Tools to launch refined attacks against embedded hardware and controller area network (CAN bus) systems are not difficult to find. Attackers could simply purchase or rent a vehicle, find its common flaws such as a backdoor in a module or network, and compromise every other vehicle in the same fleet.

Who is Responsible for Autonomous Vehicle Security?

First-party automakers are not the only ones who should be prioritizing digital safety. Third-party suppliers can also be at risk of a compromise. Attackers could find and exploit a vulnerability in a manufacturer's network. Even a flaw unrelated to the vehicle operations unit could allow them to pivot onto a supplier's network, Laurie says.

That is why it is critical that [the entire autonomous vehicle infrastructure](#) — every server, network, device, application, vehicle and component — must be protected. Just one poorly configured server on the manufacturer's or supplier's end can lead to an attacker breaking into the server, pivoting onto the backend network and gaining control of the connected application and therefore the vehicle.

New Mandate Aims To Protect Drivers and Vehicles

A new United Nations regulation, [UNECE WP29](#), should help automotive manufacturers and suppliers build security controls and processes into the autonomous vehicle lifecycle. It lists common threats, risks and attack methods. It also covers threat reduction processes and controls that automakers in countries covered by the U.N. mandate must implement to protect against the highlighted attacks. These entities must also attest that their third-party suppliers are adhering to the mandate.

Another beneficial aspect is that compliance is required for all stages of the vehicle's life — development, production and post-production. Automakers have to renew their certificate of compliance every three years. Even if they stop producing autonomous vehicles, if those vehicles are still on the market, they must comply. If they don't, they will not be allowed to sell vehicles.

The regulation states certain countries in the European Union and the Asia-Pacific region must comply. However, any entity which sells vehicles to those regions must also comply.

According to Laurie, the mandate does a good job addressing the main threats and risks. If automakers test each threat listed, they should vastly reduce their risk of a compromise. Addressing these potential problems through all stages of manufacturing helps create a baseline of autonomous vehicle cybersecurity.

To learn more about X-Force Red Automotive Testing, visit: www.ibm.com/security/services/automotive-testing.

The post [Autonomous Vehicle Security Needs From A Hacker's Perspective](#) appeared first on [Security Intelligence](#).

Source: <https://securityintelligence.com/posts/autonomous-car-security-hackers-perspective>

4. Software AG IT giant hit with \$23 million ransom by Clop ransomware

The Clop ransomware gang hit the network of German enterprise software giant Software AG last Saturday, asking for a ransom of \$23 million after stealing employee information and company documents.

[Software AG](#) is a software company headquartered in Darmstadt, Germany, with more than 5,000 employees and operations in over 70 countries around the globe.

Software AG's customer list includes organizations from government, banking, transportation, insurance, retail, and more, Airbus, Lufthansa, DHL, Telefonica, Credit Suisse, and Continental being just a small sample of the 70% of Fortune 1000 companies that use its products.

Attack affected Software AG's internal network

"The IT infrastructure of Software AG is affected by a malware attack since the evening of 3 October 2020," [says](#) a press release issued by the company on Monday.

Software AG also says that the ransomware attack only affected its internal network while customer cloud services were unaffected.

"While services to its customers, including its cloud-based services, remain unaffected, as a result, Software AG has shut down the internal systems in a controlled manner in accordance with the company's internal security regulations," the software giant adds.

"The company is in the process of restoring its systems and data in order to resume orderly operation." Software AG added that its internal communication and helpdesk services are still affected by the attack.

In a press release published three days later, on Thursday, Software AG [said](#) that it found "first evidence that data was downloaded from Software AG's servers and employee notebooks."

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at [+16469613731](tel:+16469613731) or on Wire at [@lawrenceabrams-bc](https://www.wire.com/@lawrenceabrams-bc).

Clop ransomware asks for a \$23 million ransom

The company says that this was a "malware attack" and doesn't mention any details related to ransomware in its press releases.

However, BleepingComputer was able to obtain the Software AG ransom note and a link to their chat on Clop's Tor payment site from security researcher [MalwareHunterTeam](#).

MalwareHunterTeam told BleepingComputer that they gained access to this information after finding the Clop ransomware executable used in the attack on Software AG.

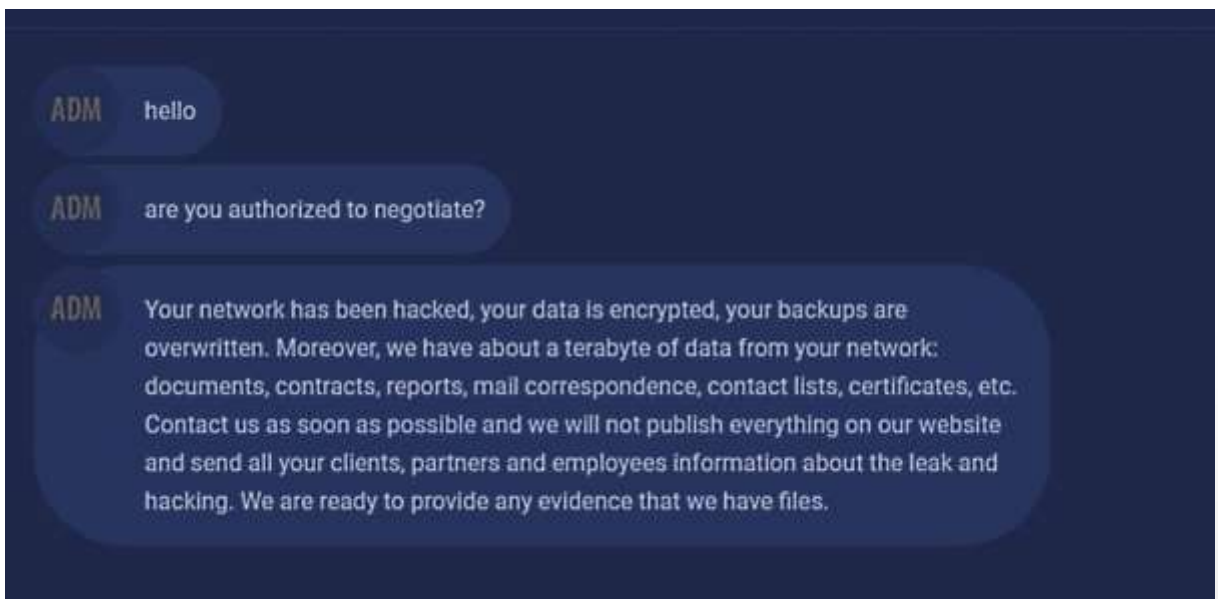
```
HELLO DEAR SOFTWARE AG
YOUR NETWORK IS ENCRYPTED!
ALL YOUR FILES ARE ENCRYPTED!
Also a lot of sensitive data has been downloaded from your network.
For example:
// [REDACTED]
This is a small part, about 10%.
If you refuse to cooperate, all data will be published for free download on our portal:
http://[REDACTED].onion/ (use TOR browser)
mirror http://[REDACTED].onion.dog/
To get access to your files back, contact us by email:
[REDACTED]
or
[REDACTED]
AND
[REDACTED]
or write to the chat at:
[REDACTED] (use TOR browser)
!!! DO NOT ATTEMPT TO RESTORE OR MOVE THE FILES YOURSELF. THIS MAY DESTROY THEM !!!
CI0p-_^
```

Software AG ransom note

The Tor payment site showing the Software AG ransom demand shows that the ransom asked by Clop for decrypting all encrypted computers on the company's network is \$23,000,000 (or 2083,0069 BTC).



According to the chat section of Clop ransomware's leak site, the attackers were able to steal information on employees' passports, health bills, and emails, also publishing a screenshot with a folder tree containing additional info potentially stolen from Software AG.



The chat on the Software AG payment site shows the Clop actors threatening to publish the entire batch of roughly 1 TB of data they claim to have stolen from Software AG's

devices including "documents, contracts, reports, mail correspondence, contact lists, certificates, etc."

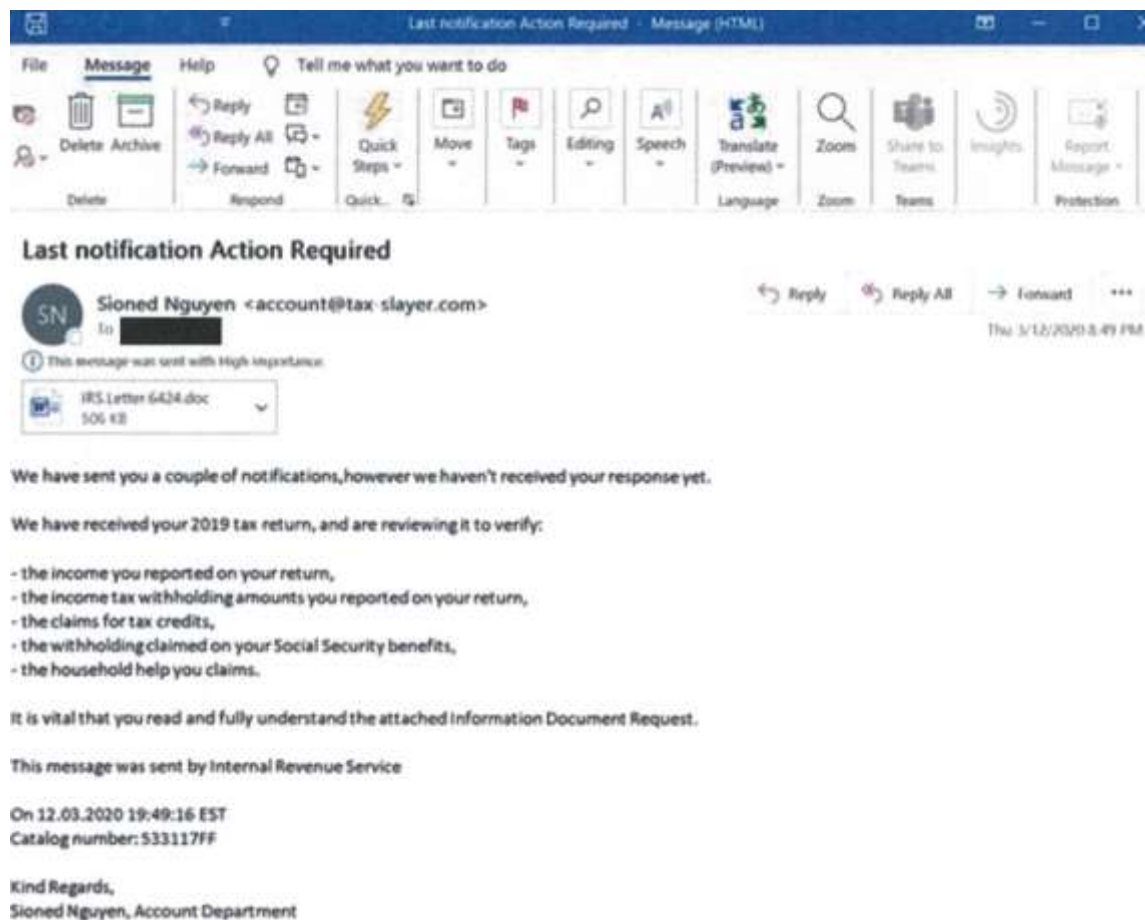
[Clop ransomware](#) was also behind the attack on [Maastricht University](#) on December 23, 2019. In February, Maastricht University confirmed that [it paid the 30 bitcoin ransom](#) requested by the Clop ransomware gang.

BleepingComputer has contacted Software AG with questions related to this attack but has not heard back at this time.

Source: <https://www.bleepingcomputer.com/news/security/software-ag-it-giant-hit-with-23-million-ransom-by-clop-ransomware/>

5. Microsoft Uses Trademark Law to Disrupt Trickbot Botnet

Microsoft Corp. has executed a coordinated legal sneak attack in a bid to disrupt the malware-as-a-service botnet **Trickbot**, a global menace that has infected millions of computers and is used to spread ransomware. A court in Virginia granted Microsoft control over many Internet servers Trickbot uses to plunder infected systems, based on novel claims that the crime machine abused the software giant's trademarks. However, it appears the operation has not completely disabled the botnet.



A spam email containing a Trickbot-infected attachment that was sent earlier this year. Image: Microsoft.

"We disrupted Trickbot through a court order we obtained as well as technical action we executed in partnership with telecommunications providers around the world," wrote **Tom Burt**, corporate vice president of customer security and trust at Microsoft, in [a blog post](#) this morning about the legal maneuver. "We have now cut off key infrastructure so those operating Trickbot will no longer be able to initiate new infections or activate ransomware already dropped into computer systems."

Microsoft's action comes just days after the U.S. military's **Cyber Command** [carried out its own attack](#) that sent all infected Trickbot systems a command telling them to disconnect themselves from the Internet servers the Trickbot overlords used to control them. The roughly 10-day operation by Cyber Command also stuffed millions of bogus records about new victims into the Trickbot database in a bid to confuse the botnet's operators.

In legal filings, Microsoft argued that Trickbot irreparably harms the company "by damaging its reputation, brands, and customer goodwill. Defendants physically alter and corrupt Microsoft products such as the Microsoft Windows products. Once infected, altered and controlled by Trickbot, the Windows operating system ceases to operate normally and becomes tools for Defendants to conduct their theft."

From the civil complaint Microsoft filed on October 6 with the **U.S. District Court for the Eastern District of Virginia**:

"However, they still bear the Microsoft and Windows trademarks. This is obviously meant to and does mislead Microsoft's customers, and it causes extreme damage to Microsoft's brands and trademarks."

"Users subject to the negative effects of these malicious applications incorrectly believe that Microsoft and Windows are the source of their computing device problems. There is great risk that users may attribute this problem to Microsoft and associate these problems with Microsoft's Windows products, thereby diluting and tarnishing the value of the Microsoft and Windows trademarks and brands."

Microsoft said it will leverage the seized Trickbot servers to identify and assist Windows users impacted by the Trickbot malware in cleaning the malware off of their systems.

Trickbot has been used to steal passwords from millions of infected computers, and reportedly to hijack access to well more than 250 million email accounts from which new copies of the malware are sent to the victim's contacts.

Trickbot's malware-as-a-service feature has made it a reliable vehicle for deploying various strains of ransomware, locking up infected systems on a corporate network unless and until the company agrees to make an extortion payment.

A particularly destructive ransomware strain that is closely associated with Trickbot — known as "Ryuk" or "Conti" — has been responsible for costly attacks on countless organizations over the past year, including healthcare providers, medical research centers and hospitals.

One recent Ryuk victim is Universal Health Services (UHS), a Fortune 500 hospital and healthcare services provider that operates more than 400 facilities in the U.S. and U.K.

On Sunday, Sept. 27, UHS shut down its computer systems at healthcare facilities across the United States in a bid to stop the spread of the malware. The disruption caused some

of the affected hospitals to redirect ambulances and relocate patients in need of surgery to other nearby hospitals.

Microsoft said it did not expect its action to permanently disrupt Trickbot, noting that the crooks behind the botnet will likely make efforts to revive their operations. But so far it's not clear whether Microsoft succeeded in commandeering all of Trickbot's control servers, or when exactly the coordinated seizure of those servers occurred.

As the company noted in its legal filings, the set of Internet address used as Trickbot controllers is dynamic, making attempts to disable the botnet more challenging.

Indeed, according to real-time information posted by [Feodo Tracker](#), a Swiss security site that tracks Internet servers used as controllers for Trickbot and other botnets, nearly two dozen Trickbot control servers — some of which first went active at beginning of this month — are still live and responding to requests at the time of this publication.

FEODO tracker by ABUSE.ch [Mitigate](#) [Browse](#) [Blocklist](#) [Statistics](#) [About](#)

- **TrickBot**: has **no** code base with Emotet. However, TrickBot usually gets dropped by Emotet for lateral movement and to drop additional malware (such as [Ryuk](#) ransomware).

IP address, AS number or AS name

Firstseen (UTC)	Host	Malware	Status	SBL	Network (ASN)	Country
2020-10-11 02:10:59	185.117.73.190	TrickBot	Online	SBL352624	AS60117 HS	NL
2020-10-11 01:50:40	195.123.240.130	TrickBot	Online	Not listed	AS204957 GREENFLOID-AS	US
2020-10-11 00:07:35	45.89.127.128	TrickBot	Online	Not listed	AS30823 COMBAHTON combahton GmbH	DE
2020-10-10 23:37:57	80.85.156.116	TrickBot	Online	Not listed	AS44493 CHELYABINSK-SIGNAL-AS	RU
2020-10-10 13:29:46	51.89.177.8	TrickBot	Online	Not listed	AS16276 OVH	GB
2020-10-10 09:31:06	45.89.127.118	TrickBot	Online	Not listed	AS30823 COMBAHTON combahton GmbH	DE
2020-10-10 09:31:06	37.220.6.115	TrickBot	Online	Not listed	AS20860 IOMART-AS	GB
2020-10-10 08:14:27	194.5.249.216	TrickBot	Online	Not listed	AS64398 NXTHOST-64398 NXTHOST.COM - NXTSERVERS SRL	RO
2020-10-10 08:14:10	45.89.127.119	TrickBot	Online	Not listed	AS30823 COMBAHTON combahton GmbH	DE
2020-10-10 07:58:29	62.108.35.36	TrickBot	Online	Not listed	AS30962 COMTRANCE-AS	DE
2020-10-10 07:47:01	51.77.112.255	TrickBot	Online	Not listed	AS16276 OVH	FR
2020-10-10 07:43:53	194.5.249.224	TrickBot	Online	Not listed	AS64398 NXTHOST-64398 NXTHOST.COM - NXTSERVERS SRL	RO
2020-10-10 07:23:44	62.108.35.29	TrickBot	Offline	Not listed	AS30962 COMTRANCE-AS	DE
2020-10-09 17:00:02	35.164.230.208	TrickBot	Offline	SBL497742	AS16509 AMAZON-02	US
2020-10-08 17:57:05	185.14.30.247	TrickBot	Online	Not listed	AS21100 ITLDC-NL	NL
2020-10-07 21:52:02	194.5.249.126	TrickBot	Online	Not listed	AS64398 NXTHOST-64398 NXTHOST.COM - NXTSERVERS SRL	RO
2020-10-06 23:29:46	185.99.2.176	TrickBot	Online	Not listed	AS200698 GLOBALHOST-BOSNIA-AS	BA
2020-10-06 15:03:51	194.5.249.136	TrickBot	Online	Not listed	AS64398 NXTHOST-64398 NXTHOST.COM - NXTSERVERS SRL	RO

Trickbot control servers that are currently online. Source: Feodotracker.abuse.ch

Cyber intelligence firm [Intel 471](#) says fully taking down Trickbot would require an unprecedented level of collaboration among parties and countries that most likely would not cooperate anyway. That's partly because Trickbot's primary command and control mechanism supports communication over [The Onion Router \(TOR\)](#) — a distributed anonymity service that is wholly separate from the regular Internet.

"As a result, it is highly likely a takedown of the Trickbot infrastructure would have little medium- to long-term impact on the operation of Trickbot," Intel 471 wrote in an analysis of Microsoft's action.

What's more, Trickbot has a fallback communications method that uses a decentralized domain name system called [EmerDNS](#), which allows people to create and use domains that cannot be altered, revoked or suspended by any authority. The highly popular cybercrime store [Joker's Stash](#) — which sells millions of stolen credit cards — also uses this setup.

From the Intel 471 report [malicious links and IP address defanged with brackets]:

"In the event all Trickbot infrastructure is taken down, the cybercriminals behind Trickbot will need to rebuild their servers and change their EmerDNS domain to point at their new servers. Compromised systems then should be able to connect to the new Trickbot infrastructure. Trickbot's EmerDNS fall-back domain safetrust[.]bazar recently resolved to the IP address 195.123.237[.]156. Not coincidentally, this network neighborhood also hosts Bazar malware control servers."

"Researchers previously attributed the development of the Bazar malware family to the same group behind Trickbot, due to code similarities with the Anchor malware family and its methods of operation, such as shared infrastructure between Anchor and Bazar. On Oct. 12, 2020 the fall-back domain resolved to the IP address 23.92.93[.]233, which was confirmed by Intel 471 Malware Intelligence systems to be a Trickbot controller URL in May 2019. This suggests the fall-back domain is still controlled by the Trickbot operators at the time of this report."

Intel 471 concluded that the Microsoft action has so far has done little to disrupt the botnet's activity.

"At the time of this report, Intel 471 has not seen any significant impact on Trickbot's infrastructure and ability to communicate with Trickbot-infected systems," the company wrote.

The legal filings from Microsoft are available [here](#).

Update, 9:51 a.m. ET: Feodo Tracker now lists just six Trickbot controllers as responding. All six were first seen online in the past 48 hours. Also added perspective from Intel 471.

Source: <https://krebsonsecurity.com/2020/10/microsoft-uses-copyright-law-to-disrupt-trickbot-botnet/>

6. Windows Update can be abused to execute malicious programs

The Windows Update client has just been added to the list of living-off-the-land binaries (LoLBins) attackers can use to execute malicious code on Windows systems.

[LoLBins](#) are Microsoft-signed executables (pre-installed or downloaded) that can be abused by threat actors to evade detection while downloading, installing, or executing malicious code.

They can also be used by attackers in their efforts to bypass Windows User Account Control (UAC) or Windows Defender Application Control (WDAC) and to gain persistence on already compromised systems.

Malicious code execution using malicious DLLs

The WSUS / Windows Update client (wuaclt) is a utility located at %windir%\system32\ that provides users partial control over some of the Windows Update Agent's functionality from the command-line.

It allows checking for new updates and installing them without having to use the Windows user interface but instead triggering them from a Command Prompt window.

Using the /ResetAuthorization option allows initiating a manual update check either on the locally configured WSUS server or via the Windows Update service [according to Microsoft](#).

However, MDSec researcher [David Middlehurst discovered](#) that wuaclt can also be used by attackers to execute malicious code on Windows 10 systems by loading it from an arbitrary specially crafted DLL with the following command-line options:

```
wuaclt.exe /UpdateDeploymentProvider [path_to_dll] /RunHandlerComServer
```

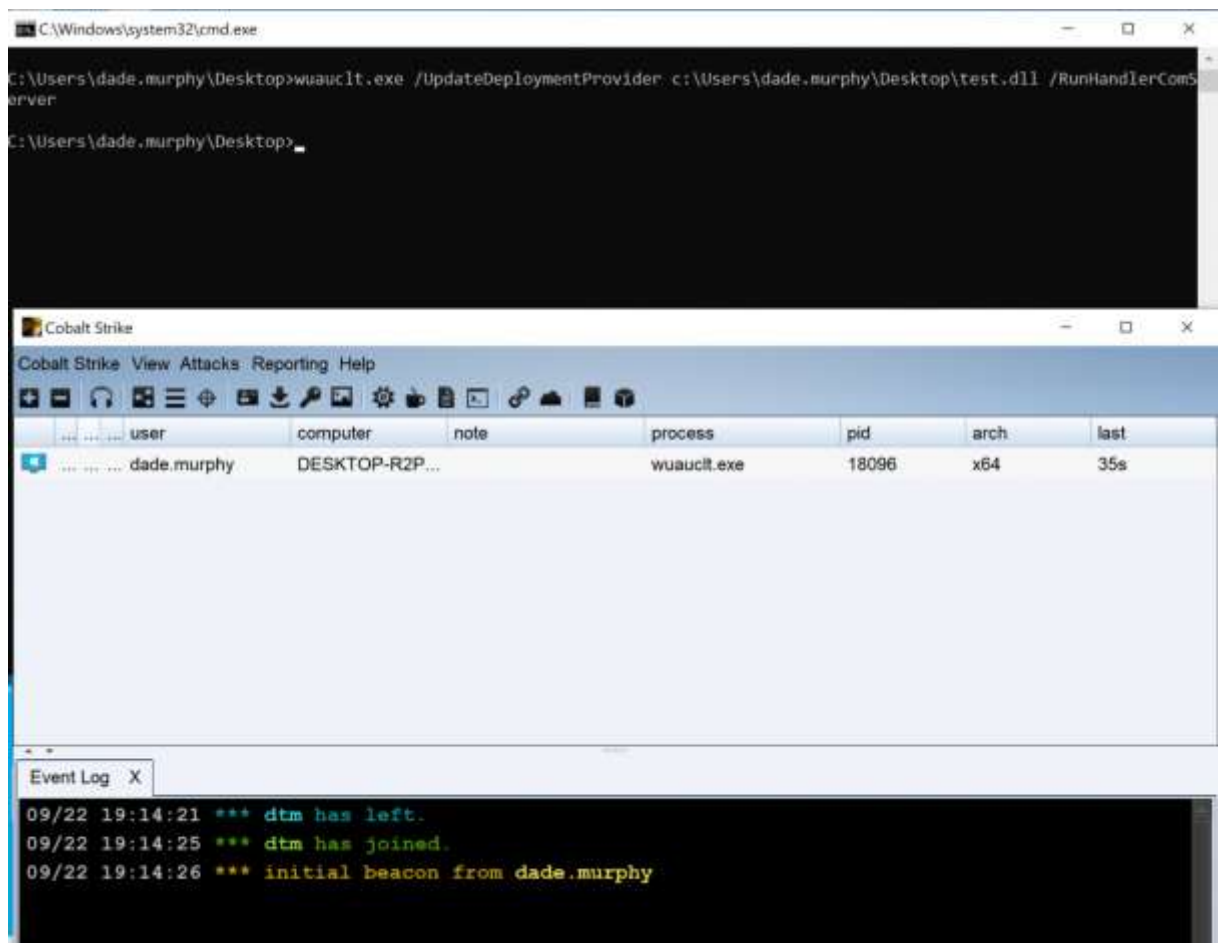


Image: David Middlehurst

As seen in the screenshot above, the Full_Path_To_DLL is the absolute path to the attacker's specially crafted DLL file that would execute code on attach.

This defense evasion technique is categorized by MITRE ATT&CK as [Signed Binary Proxy Execution via Rundll32](#) and it enables attackers to bypass anti-virus, application control, and digital certificate validation protection

In this case, it does it by executing malicious code from a DLL loaded using a signed-Microsoft binary, the Windows Update client (wuauclt).

After discovering that wuauclt can also be used as a LoLBin, Middlehurst also [found a sample](#) using it in the wild.

Microsoft recently updated the Windows 10 Microsoft Defender antivirus solution, ironically and quietly adding a way to [download files \(potentially malicious\) onto Windows devices](#).


```

Command Prompt

[-ReturnHR]

-Trace [-Grouping #] [-Level #]           Scans for malicious software
-GetFiles [-SupportLogLocation <path>]     Starts diagnostic tracing
-GetFilesDiagTrack                         Collects support information
                                           Same as Getfiles but outputs to
                                           temporary DiagTrack folder
-RemoveDefinitions [-All]                 Restores the installed
                                           signature definitions
                                           to a previous backup copy or to
                                           the original default set of
                                           signatures
                                           [-Engine]                             Restore the installed engine to
                                           the previous version saved
                                           [-DynamicSignatures]               Removes only the dynamically
                                           downloaded signatures
-SignatureUpdate [-UNC | -MMPC]           Checks for new definition updates
-Restore [-ListAll | [[-Name <name>] [-All] | [-FilePath <filePath>]] [-Path <path>]] Restore or list
                                           quarantined item(s)
-AddDynamicSignature [-Path]              Loads a dynamic signature
-ListAllDynamicSignatures                 List the loaded dynamic signatures
-RemoveDynamicSignature [-SignatureSetID] Removes a dynamic signature
-CheckExclusion -path <path>               Checks whether path is excluded
-DownloadFile -URL <url> -path <path>     Downloads a file from the given URL
                                           to the location given in path. Path
                                           should also have the file name in it.

Additional Information:
Support information will be in the following directory:
C:\ProgramData\Microsoft\Windows Defender\Support

```

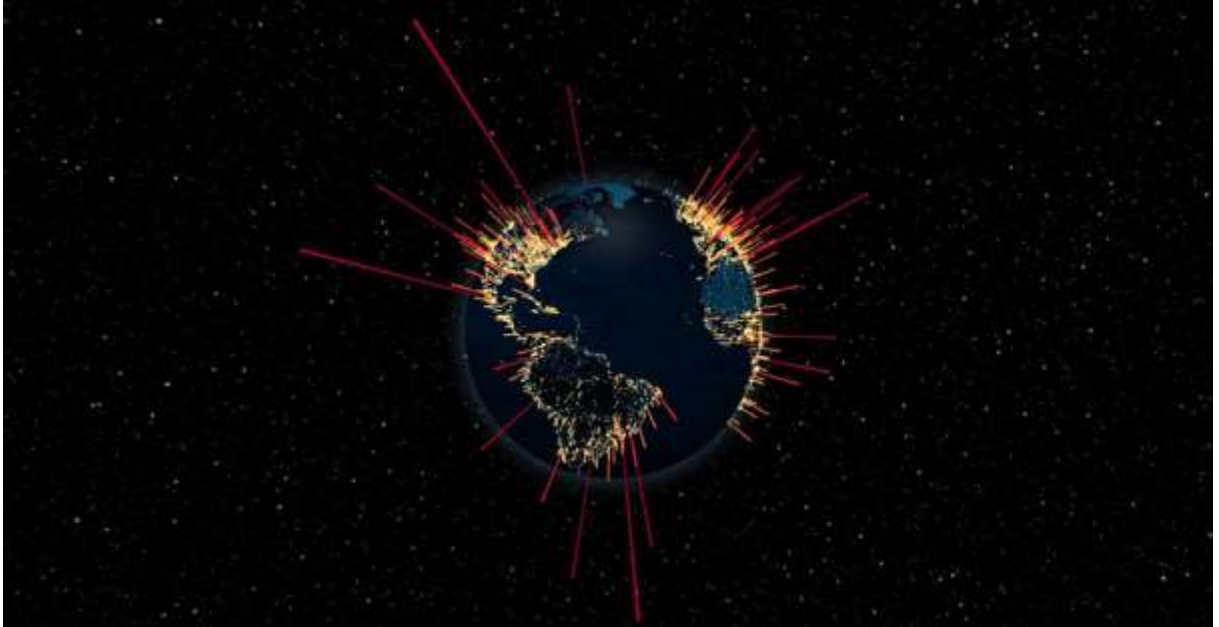
MpCmdRun help

Microsoft [later removed](#) the capability from MpCmdRun.exe (the Microsoft Antimalware Service Command Line Utility).

Last month, BleepingComputer also reported that the Microsoft Windows TCPIP Finger command can also be used as a file downloader and as a [substitute command and control \(C3\) server for exfiltrating data](#).

Source: <https://www.bleepingcomputer.com/news/security/windows-update-can-be-abused-to-execute-malicious-programs/>

7. Nation-state actor hit Google with the largest DDoS attack



In an overview of distributed denial-of-service (DDoS) trends targeting its network links, Google revealed that in 2017 a nation-state actor used massive firepower that amounted to more than 2.7 terabits per second.

The actor targeted thousands of Google IP addresses at the same time and used several attack methods in a campaign that span across multiple months.

Google [did not attribute the attack](#) to a particular actor but said that the bad UDP packets hurled at its systems came from devices using several Chinese internet service providers (ASNs 4134, 4837, 58453, and 9394).

In an analysis of DDoS trends over the last years, Damian Menscher, a Security Reliability Engineer for Google Cloud, said that the attack occurred in September 2017 and used 180,000 exposed CLDAP, DNS, and SMTP servers to amplify responses directed at Google.

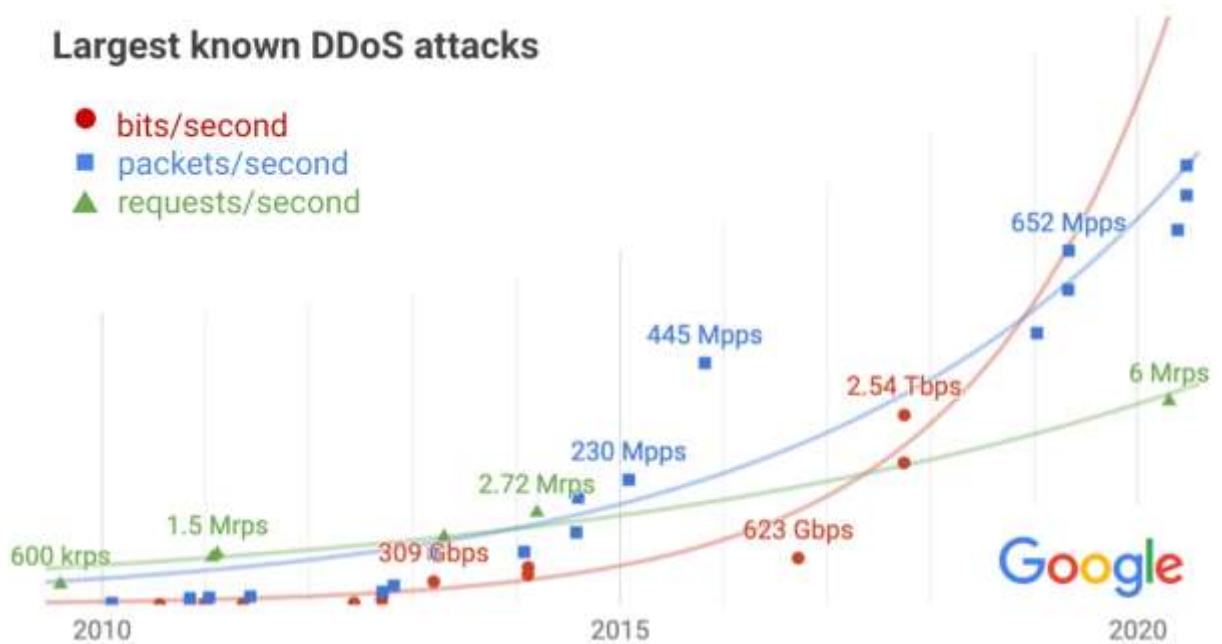
The effort, large as it was, did not create problems and Google services and infrastructure remained unscathed.

"Despite simultaneously targeting thousands of our IPs, presumably in hopes of slipping past automated defenses, the attack had no impact" - [Damian Menscher](#)

Menscher says that the size of the attack, which is the largest ever disclosed publicly, shows "the volumes a well-resourced attacker can achieve," noting that it was four times larger than the Mirai DDoS attack that shook the internet in 2016.

Another large attack was recorded this year from an IoT botnet. It targeted the network protocol and hit with 690 million packets per second (mpps)

Largest known DDoS attacks



In a [report](#) at the beginning of the year, Amazon AWS reported a 2.3Tb per second volumetric DDoS attack, recorded in the first quarter of 2020.

The largest packet rate per second mitigated by Amazon in that period was 293.1 Mpps, more than two times smaller than the one Google recorded this year.

Google warns that while its report shows the scale of past and current DDoS attacks and can help predict the size of future ones, defenses must be over-provisioned so they can withstand attacks of unexpected sizes.

Collaborating with partners in the internet community (network providers, vendors, customers) can help mitigate large attacks in a timely manner. Network providers can trace bad packets and filter them, vendors can provide patches and alert customers to apply them.

As the internet keeps growing, it provides resources to both adversaries and defenders. Knowing what to expect, defenders can determine the capacity they need to resist the largest attacks.

Source: <https://www.bleepingcomputer.com/news/security/nation-state-actor-hit-google-with-the-largest-ddos-attack/>

8. Watch out for Emotet malware's new 'Windows Update' attachment

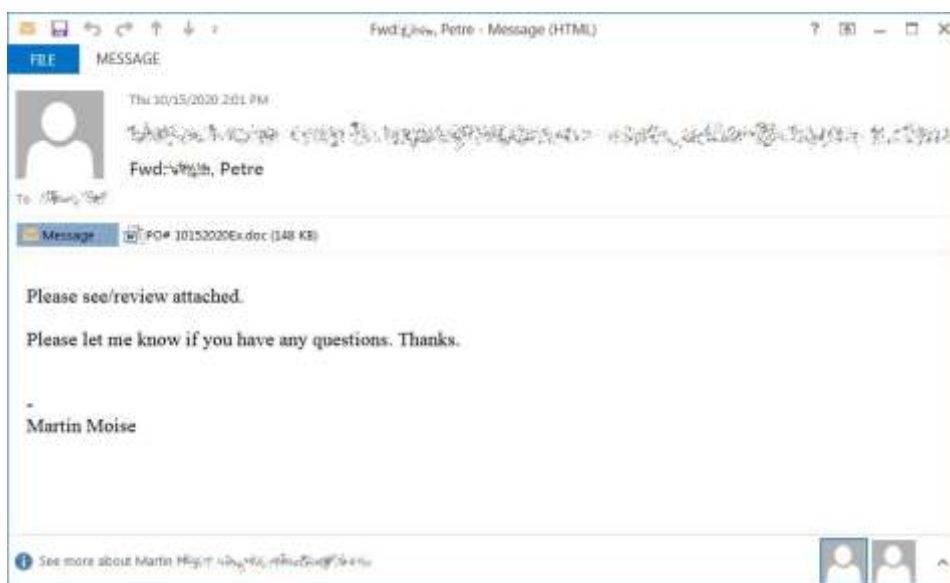


The Emotet botnet has begun to use a new malicious attachment that pretends to be a message from Windows Update telling you to upgrade Microsoft Word.

Emotet is a malware infection that spreads through spam emails containing malicious Word or Excel documents. These documents utilize macros to download and install the Emotet Trojan on a victim's computer, which uses the computer to send spam email and [ultimately leads to a ransomware attack](#) on a victim's network.

After a short vacation, the Emotet malware returned to operation on October 14th and began blasting out malicious spam worldwide.

These spam campaigns pretend to be invoices, shipping information, [COVID-19 information](#), [information about President Trump's health](#), resumes, or purchase orders, as shown below.



Example Emotet spam email

Attached to these spam emails are malicious Word (.doc) attachments or links to download one.

When opened, these attachments will prompt a user to 'Enable Content' so that malicious macros will run to install the Emotet malware on a victim's computer.

To trick users into enabling the macros, Emotet uses various document templates, including pretending to be created on iOS devices, Windows 10 Mobile, or that the document is protected.

With its return to activity, Emotet switched to a new template that pretends to be a message from Windows Update stating that Microsoft Word needs to be updated before the document can be viewed.

Windows Update

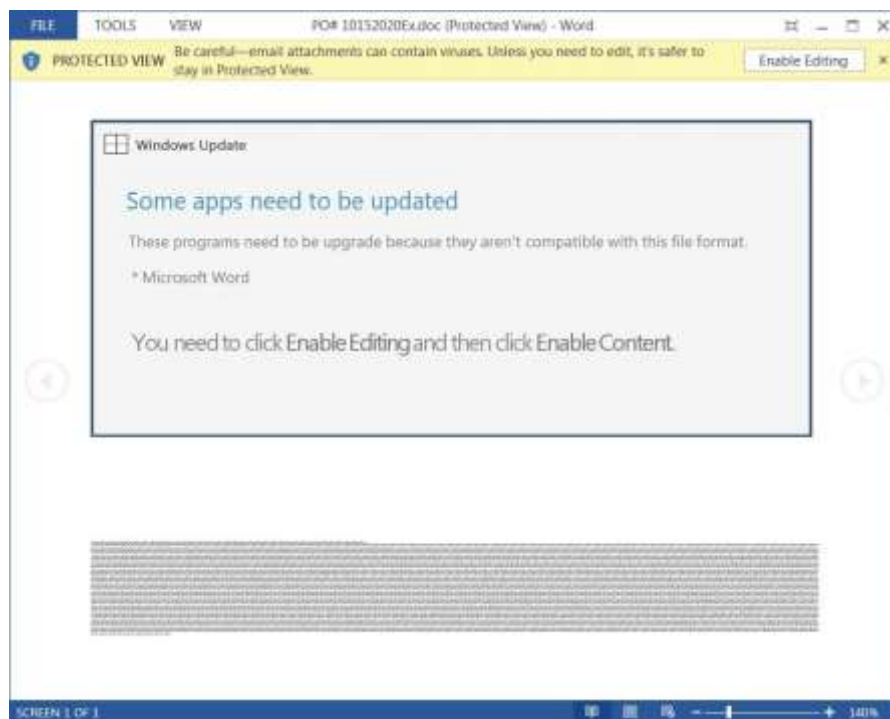
Some apps need to be updated

These programs need to be upgrade because they aren't compatible with this file format.

* Microsoft Word

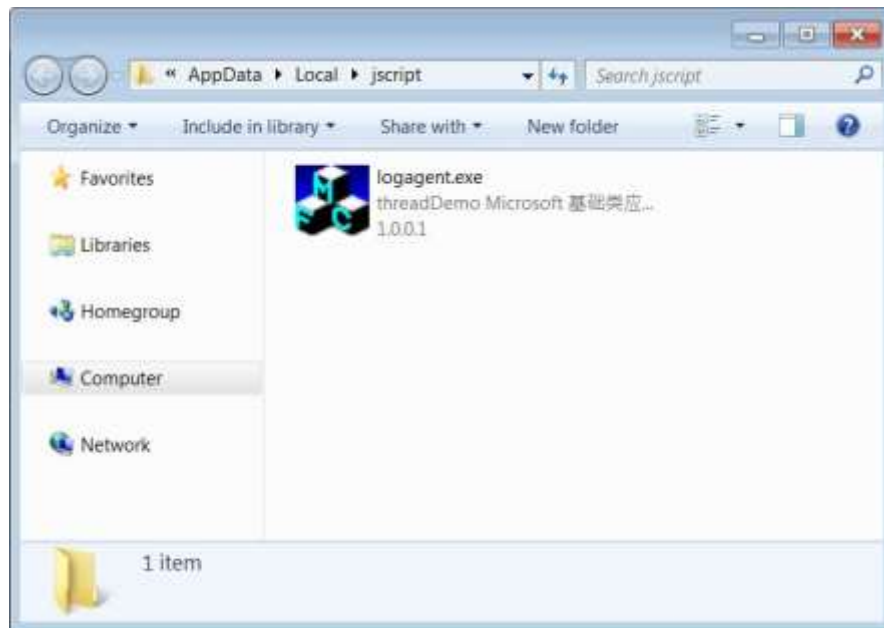
You need to click Enable Editing and then click Enable Content.

To update Word, the message tells the user to click on the Enable Editing and Enable Content buttons, which will cause the malicious macros to fire off,



New 'Windows Update' Emotet attachment

These malicious macros will download and install the Emotet malware on a victim's computer, as shown below.

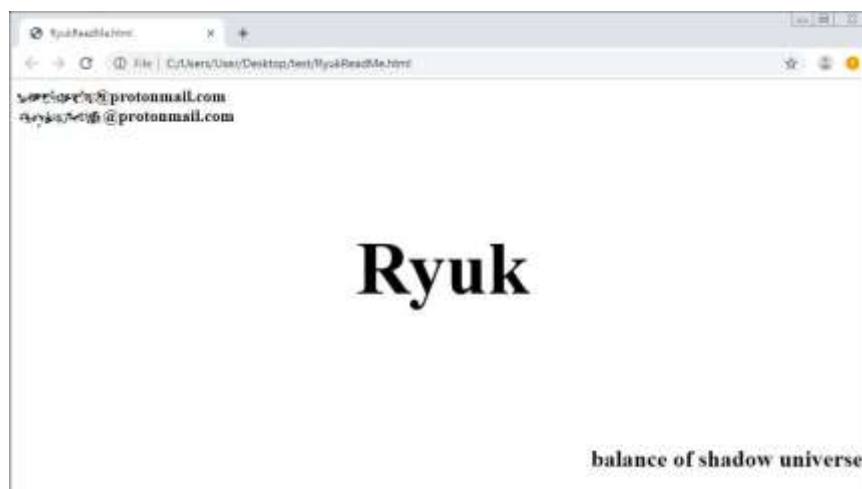


Emotet malware installed in Windows

Why it's necessary to recognize Emotet attachments?

Emotet is considered the most [widely spread malware](#) targeting users today. It is also particularly dangerous as it installs other malware such as Trickbot and QBot onto a victim's computer.

While TrickBot and QBot perform malicious activity on their own, such as stealing stored passwords, banking information, and assorted other information, they also commonly lead to [Conti \(TrickBot\)](#) or [ProLock \(QBot\)](#) ransomware attacks.



Ryuk ransom note

Due to this, it is vital to recognize the malicious document templates used by Emotet so that you do not accidentally become infected.

Source: <https://www.bleepingcomputer.com/news/security/watch-out-for-emotet-malwares-new-windows-update-attachment/>

9. Rapper Scams \$1.2M in COVID-19 Relief, Gloats with 'EDD' Video

"Nuke Bizzle" faces 22 years in prison after brazenly bragging about an identity-theft campaign in his music video, "EDD."

Rapper Fontrell Antonio Baines, who goes by the stage name "Nuke Bizzle," made his first appearance in U.S. District Court in downtown Los Angeles on Friday after being charged with fraudulently applying for more than [\\$1.2 million in jobless benefits](#) under the Coronavirus Aid, Relief and Economic Security Act (CARES Act), according to a statement from the U.S. Attorney's Office in the Central District of California.

Allegedly, Baines was able to defraud the California Employment Development Department (EDD) into distributing CARES Act relief payments under the Pandemic Employment Assistance (PUA) provision, the statement from the U.S. Attorney's office said. The PUA is intended to aid independent contractors who aren't typically eligible for unemployment benefits.

Prosecutors claimed he used the names of identity-theft victims to get debit cards issued and mailed to various addresses in the Beverly Hills and Koreatown neighborhoods of Los Angeles, the statement added.

He is charged with three felonies: Access device fraud, aggravated identity theft and interstate transportation of stolen property. If convicted of all of them, Baines would face a statutory maximum sentence of 22 years in federal prison.

EDD Music Video Tipoff

Authorities were tipped off to the scheme after [Baines posted a music video](#) on YouTube and Instagram titled "EDD," an apparent reference to the state unemployment agency.

In the video, posted on Sept. 11 and also featuring rapper Fat Wizza, Baines brags about "my swagger for EDD," and holds up a stack of envelopes from the office, adding, "You gotta sell cocaine, I just file a claim."



Source: YouTube.

The video shows Nuke Bizzle and Fat Wizza collecting EDD envelopes from various mailboxes, filing fraudulent claims on a laptop and spending wads of cash.

Apparently, the video's disclaimer that "this video was created with props and was made for entertainment purposes only" wasn't enough to dissuade authorities from taking a closer look at the ode to EDD.

An investigation by the U.S. Department of Labor Office of Inspector General, the U.S. Postal Service, the IRS and California Employment Development Dept. found that Baines allegedly accessed more than \$704,000 through 92 debit cards issued by EDD, with more than \$1.2 million in benefits available. The statement added the money was used for cash withdrawals and purchases, including in Las Vegas, where Baines was arrested on Sept. 23.

At the time of his arrest, Baines was reported to have been holding eight debit cards issued under seven separate names.

Widespread CARES Act Fraud

Rampant [fraud directed at the CARES Act](#) and COVID-19 relief has been going on since the more than \$2 trillion economic assistance bill passed on March 27 to aid families and businesses impacted by the pandemic.

In April, the Small Business Administration (SBA) was [breached, exposing the information](#) of 8,000 businesses which had applied for loans to weather COVID-19, including Social Security numbers, Tax ID numbers, financial information and much more.

In May, the business email compromise (BEC) gang known as Scattered Canary submitted [hundreds of fake claims](#) across several states with personal data that Agari researchers said looked like was lifted from stolen W2 tax forms. The group reportedly received almost 50 prepaid debit cards issued by Green Dot.

[BEC attacks](#) typically involve a scammer impersonating a trusted source from within a company, with the intention of tricking someone to wire money or share other sensitive data.

Overall, the CARES Act has driven a sharp uptick in [phishing and other schemes](#) to get ahold of American taxpayer data and an easy payout. Secureworks CTU reported in May seeing ads with phony tax forms to trick users out of their information, as well as emails impersonating the IRS to "confirm" information to receive stimulus payments.

Baines put out a video bragging about the alleged crime and showing how it worked. But as the case works its way through the courts, a reminder from the U.S. Attorney's office reads, "Every defendant is presumed innocent until and unless proven guilty beyond a reasonable doubt."

Source: <https://threatpost.com/rapper-scams-covid-19-relief-video/160315/>

10. French IT giant Sopra Steria hit by Ryuk ransomware

French IT services giant Sopra Steria suffered a cyberattack on October 20th, 2020, that reportedly encrypted portions of their network with the Ryuk ransomware.

Sopra Steria is a European information technology company with 46,000 employees in 25 countries worldwide. The company provides a wide range of IT services, including consulting, systems integration, and software development.

On October 21st, Sopra Steria [issued a statement](#) that they had suffered a cyberattack on the evening of October 20th, but provided few details about the attack.

"A cyberattack has been detected on Sopra Steria's IT network on the evening of 20th October.

Security measures have been implemented in order to contain risks.

The Group's teams are working hard for a return to normal as quickly as possible and every effort has been made to ensure business continuity.

Sopra Steria is in close contact with its customers and partners, as well as the competent authorities."

Reported Ryuk ransomware attack

A source familiar with the attack has told BleepingComputer that the Sopra Steria network was encrypted by Ryuk ransomware, the same group that [infected the Universal Health Services](#).

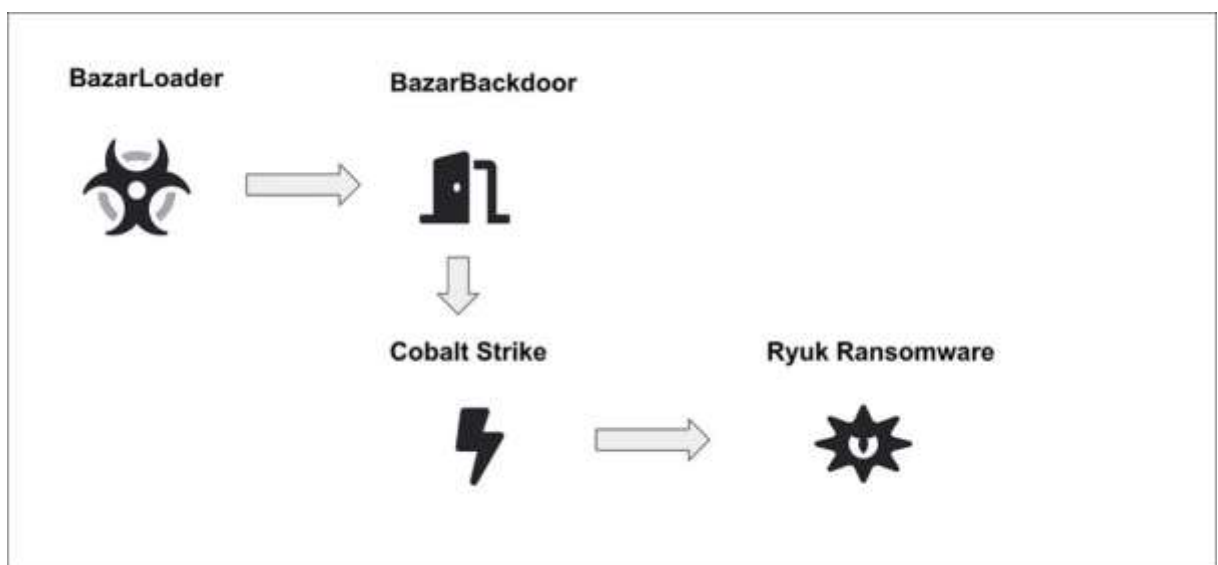
Numerous sources have also told the French IT website [LeMagIT](#) that it was Ryuk ransomware threat actors who were behind the attack.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at [+16469613731](tel:+16469613731) or on Wire at @lawrenceabrams-bc.

This hacking group is known for its [TrickBot](#) and [BazarLoader](#) infections that allow threat actors to access a compromised network and deploy the Ryuk or Conti ransomware infections.

BazarLoader is increasingly being used in Ryuk attacks against high-value targets due to its stealthy nature and is less detected than TrickBot by security software.

When installed, BazarLoader will allow threat actors to remotely access the victim's computer and use it to compromise the rest of the network.



BazarBackdoor attack flow
Source: Advanced Intel

After gaining access to a Windows domain controller, the attackers then [deploy the Ryuk ransomware](#) on the network to encrypt all of its devices, as illustrated in the diagram above.

When we reached out to Sopra Steria for further confirmation, we were told that they "don't have further details to share."

Source: <https://www.bleepingcomputer.com/news/security/french-it-giant-sopra-steria-hit-by-ryuk-ransomware/>

11. The Importance of Good Cyber Hygiene — Now More than Ever

It may feel too simplistic to be talking about cyber hygiene with CISOs. But in my years as a threat researcher, and now running a global team of threat researchers, data analysts, and forensics experts, I can say authoritatively that the lack of consistent cyber hygiene is the largest and most persistent threat inside most organizations. And the risk continues to grow as organizations continue to grow their networks and expand their attack surfaces without a holistic security architecture or management system in place.

The concept of cyber hygiene is a deceptively simple one: It involves a series of practices and precautions that, when repeated regularly, keep us safe and our devices working as they should. But that's easier said than done with distributed networks, IoT everywhere, the adoption of multi-cloud infrastructures, and a growing reliance on SaaS application usage. Add the convergence of IT and OT, and the number of aging devices that cannot be taken offline because they monitor or manage critical systems 24x7, and the risks are greater, and the table stakes are higher, than ever before.

Keeping Remote Workers Safe

One of the most critical places on which to focus cyber hygiene efforts is remote workers. The rapid growth in a [mobile workforce](#) and their reliance on personal devices and home networks is just the latest example of the challenges that IT teams face. Unfortunately, enforcing cyber hygiene for remote workers seems to be low on the list for overworked IT teams – somewhere below keeping the business up and running and ensuring access to business applications and essential resources.

Of course, the challenge is that employees working from home are using unsecured personal devices, from laptops to smartphones to tablets, to stay connected during the workday. And these devices, attached to weaker and far more vulnerable home networks, have created the perfect platform from which cyber criminals can launch [attacks](#) on enterprise data.

Over the past several months, cybercriminals have combined social engineering tactics that exploit fears about the Covid-19 pandemic with older exploits targeting unpatched vulnerabilities found in devices deployed in many home networks. They have also modified their strategies, switching from email-based attacks, which many remote users have been trained to avoid, to new browser-based attack vectors. And once the corporate network has been breached, cybercriminals are delivering new, more malicious strains of ransomware and other malware.

Adapting to the Post-Pandemic Threat Landscape

While 2020 is currently on track to break the record for the number of vulnerabilities identified and published in a single year, these vulnerabilities also have the lowest rate of exploitation ever observed in the 20-year history of the CVE (Common Vulnerabilities and Exposures) list. Instead, vulnerabilities from 2018 have claimed the highest exploitation prevalence (65%). And more than 25% of firms have reported attempts to exploit CVEs from 2005. At the same time, exploits targeting consumer-grade routers and IoT devices have been among FortiGuard Labs' top IPS detections according to our research. While some of these target newer vulnerabilities, a staggering volume have targeted exploits first discovered in 2014.

The critical lesson is this: Do not assume that older vulnerabilities, including those more than 15 years old, cannot cause problems.

What these trends show is that cybercriminals are extremely agile. Within days of seeing that companies were switching workers to remote status, the dark web was filled with phishing exploits targeting novice workers. Within weeks, threat sensors saw a dramatic drop off in threats targeting corporate resources and a corresponding spike in new attacks targeting consumer-grade routers, personal devices, gaming systems, and other devices connected to home networks. Cybercriminals are clearly more than willing to put in the work to find vulnerabilities that still exist within home networks that can then be used to enter the corporate network. Of course, many of these attacks are based on the same bad tricks these criminals have relied upon for years simply because they work. With this in mind, organizations must do two things. First, act swiftly to inform employees about cyber hygiene practices. And second, prepare them and their defenses to repel traditional threats like phishing scams and ransomware attacks, as well as new browser-based web attacks, especially as they continue to work remotely. Hosting video conferences to spread cybersecurity awareness across all arms of the business, sending out regular email updates, and urging employees to keep an eye out for unusual or suspicious emails and webpages are just a few examples of the initial steps to take.

Top 10 Cyber Hygiene Tips to Employ Right Now

Thankfully, despite the continued prevalence of ransomware and the spike in HTML/phishing attacks, there are a number of simple steps organizations and their employees can take to build a stronger barrier against threats. Some of these steps are as simple as creating stronger passwords and performing regular software and application updates. Others may require the addition of newer, more advanced endpoint security software.

It's also important to note that certain types of business resources are at particularly high-risk for attacks in the current climate. These include financial systems, customer support systems, and research and development resources. Extra measures and precautions may

need to be taken beyond the steps outlined below to protect these sensitive, high-priority assets.

- Ensure all employees receive substantial training, both when hired and periodically throughout their tenure, on how to spot and report suspicious cyber activity, maintain cyber hygiene, and now, on how to secure their personal devices and home networks. By educating individuals, especially remote workers, on how to maintain cyber distance, stay wary of suspicious requests, and implement basic security tools and protocols, CISOs can build a baseline of defense at the most vulnerable edge of their network that can help keep critical digital resources secure. This can involve online learning and workshops with experts.
- Run background checks before designating [power users](#) or granting privileged access to sensitive digital resources. By taking this extra step, organizations can make informed decisions that will inherently mitigate the risks associated with insider threats.
- Keep all servers, workstations, smartphones, and other devices used by employees up to date by applying frequent security updates. Ideally, this process should be automated, and enough time allowed for updates to be vetted in a testing environment. Proximity controls, such as cloud-based access controls and secure web gateways, can help secure those remote devices that cannot be updated or patched.
- Install anti-malware software to stop a large majority of attacks, including phishing scams and attempts to exploit known vulnerabilities. Try to invest in tools that offer sandboxing functionality (whether as part of an installed security package or as a cloud-based service) to detect [Zero-Day](#) and other unknown threats. New Endpoint Detection and Response (EDR) tools should be on every CISO's shopping list as they are not only very effective at not only repelling malware but can also identify and disable malware that manages to bypass perimeter controls before they can execute their payloads.
- Ensure an incident response/recovery plan is in place, including a hotline through which employees can promptly report a suspected breach, even when they are working from home. This way, in the event of an attack, downtime will be minimized, and employees will already be familiar with critical next steps.
- Use [secure access points](#), whether physical or cloud-based, and create a secured and segmented network for employees to utilize when connecting remotely. VPNs allow organizations to extend the private network across public Wi-Fi using an encrypted virtual point-to-point connection; this both enables and maintains secure remote access to corporate resources. And a zero trust network access strategy that includes NAC and network segmentation should also be in place.

- Implement a strong [access management](#) policy, requiring multi-factor authentication when possible and maintaining strict standards for [password creation](#). Employees should not be allowed to reuse passwords across networks or applications, whether corporate or personal, and should be encouraged to set complex passwords with various numbers and special characters. Consider providing password management software so they can keep track of passwords.
- Encrypt data in motion, in use, and at rest. However, VPN and other encrypted tunnels can also be used to securely inject malware and exfiltrate data. Which means that organizations need to invest in technologies that can inspect encrypted data at business speeds as well as monitor data access, file transfers, and other significant activity.
- Keeping up with the speed and volume of attacks can scale well beyond the limitations of human security analysts. As a result, machine learning and AI-driven security operations are no longer optional. They enable organizations to see and protect data and applications across thousands or millions of users, systems, devices, and critical applications—even across different network environments, such as multi-cloud, and the full range of network edges, including LAN, WAN, data center, cloud, and remote worker edges.
- For security solutions to be as agile as the networks they need to protect (and the cybercriminals they need to defend against), they need actionable updates to keep pace with the [shifting threat landscape](#). This means that even the fastest and most adaptable security solutions are only as effective as the threat intelligence infrastructure and researchers that support them.

Final Thoughts on Good Cyber Hygiene

In the wake of COVID-19, CISOs have been faced with a seemingly impossible task: Keep enterprise networks secure while employees continue to work from home, perhaps indefinitely. And they have needed to do so on a limited budget, fewer resources, and a team of security professionals that's already stretched thin. The solution? Enact an organization-wide cyber hygiene protocol, building the remote network security infrastructure from the ground up. By focusing on training, awareness, and education, employees will be better able to perform basic security tasks such as updating devices, identifying suspicious behaviors, and practicing good cyber hygiene across teams. After that, it is essential that organizations invest in the right systems and solutions – from VPNs to anti-malware software and encryption technologies – that enable clear visibility and granular control across the entire threat landscape. Complexity is the enemy of security, so the best response to an increasingly complicated and highly dynamic digital world is to get back to the basics. And that starts with cyber hygiene.

Source: <https://www.fortinet.com/blog/ciso-collective/the-importance-of-good-cyber-hygiene-now-more-than-ever>

12. Google employees personal info exposed in law firm data breach

Immigration law firm Fragomen, Del Rey, Bernsen & Loewy, LLP has disclosed a data breach that exposed current and former Google employees' personal information.

Fragomen is one of the USA's largest law firms covering immigration law, with over 582 attorneys in 47 locations worldwide.

Data breach exposes US employment forms

In a "Notice of Data Breach" sent to Googlers impacted by the breach, Fragomen states that they are responsible for providing I-9 employment verification services to Google.

According to the notification, the law firm recently learned that their network was compromised, and the hacker accessed a file containing Googler's personal information.

"We recently became aware of suspicious activity within our computer network. While our investigation is ongoing, we discovered that an unauthorized third party gained access to a single file containing personal information relating to I-9 employment verification services. This file contained personal information for a discrete number of Googlers (and former Googlers), including you," the [data breach notification](#) stated.

A [Form I-9](#) must be filled out by all US employees to declare their citizenship and eligibility to work in the United States.

This form contains information that could include an employee's full name, mailing address, date of birth, email address, phone number, social security number, passport numbers, and other immigration identifiers.

As this information is very sensitive and can be used by malicious actors for identity theft or other malicious activity, any Googlers affected should be on the lookout for spear-phishing attempts or fraudulent activity on their credit reports.

Fragomen is offering one year of free credit monitoring to all affected Googlers.

BleepingComputer has contacted both Google and Fragomen with questions on the number of people affected and how the attack occurred but has not heard back.

Source: <https://www.bleepingcomputer.com/news/security/google-employees-personal-info-exposed-in-law-firm-data-breach/>

13. Enel Group hit by ransomware again, Netwalker demands \$14 million

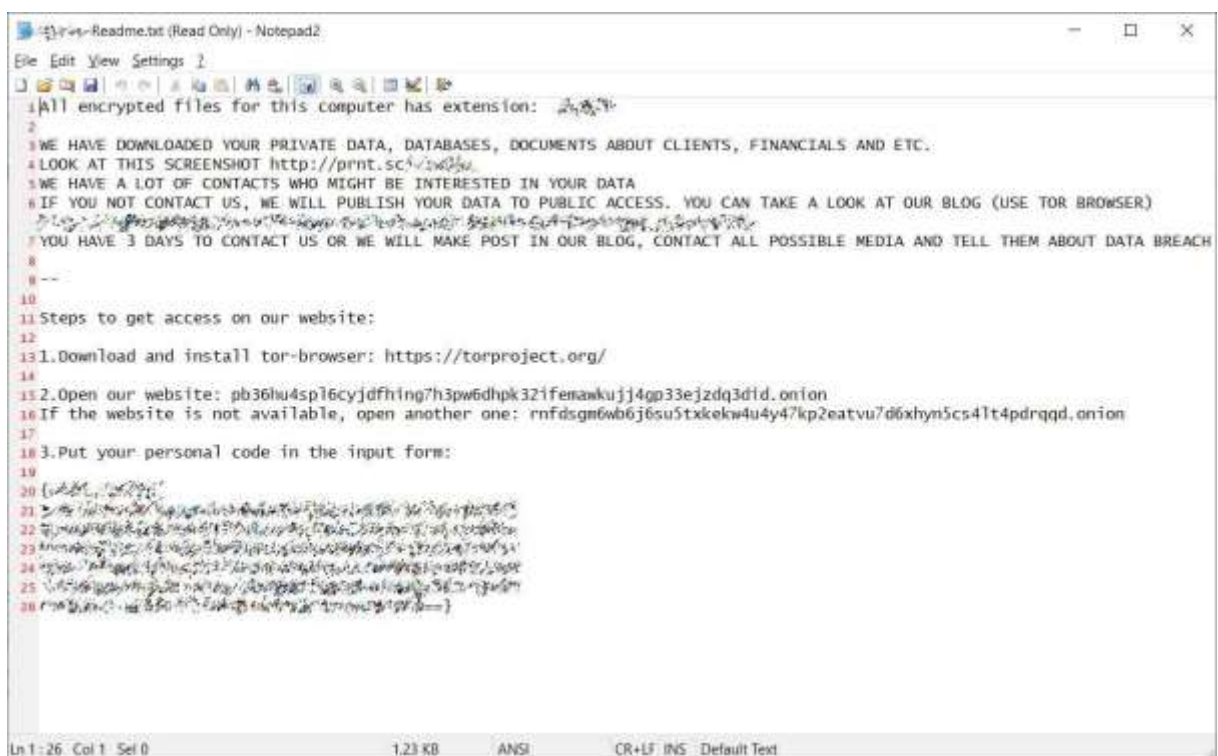
Multinational energy company Enel Group has been hit by a ransomware attack for the second time this year. This time by Netwalker, who is asking a \$14 million ransom for the decryption key and to not release several terabytes of stolen data.

Enel is one of the largest players in the European energy sector, with more than 61 million customers in 40 countries. As of August 10, it ranks 87 in Fortune Global 500, with a revenue of almost \$90 billion in 2019.

Enel hit with Netwalker Ransomware attack

In early June, Enel's internal network was [attacked by Snake ransomware](#), also referred to as EKANS, but the attempt was caught before the malware could spread.

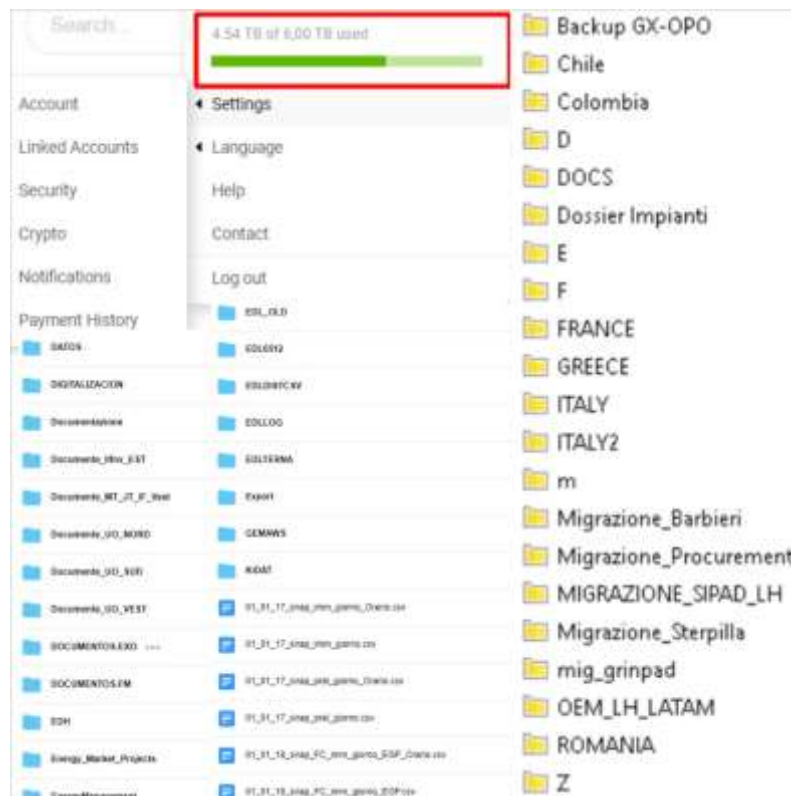
On October 19th, a researcher shared a Netwalker ransom note with BleepingComputer that appeared to be from an attack on Enel Group.



```
1 All encrypted files for this computer has extension: .NET
2
3 WE HAVE DOWNLOADED YOUR PRIVATE DATA, DATABASES, DOCUMENTS ABOUT CLIENTS, FINANCIALS AND ETC.
4 LOOK AT THIS SCREENSHOT http://prnt.sc/...
5 WE HAVE A LOT OF CONTACTS WHO MIGHT BE INTERESTED IN YOUR DATA
6 IF YOU NOT CONTACT US, WE WILL PUBLISH YOUR DATA TO PUBLIC ACCESS. YOU CAN TAKE A LOOK AT OUR BLOG (USE TOR BROWSER)
7 YOU HAVE 3 DAYS TO CONTACT US OR WE WILL MAKE POST IN OUR BLOG, CONTACT ALL POSSIBLE MEDIA AND TELL THEM ABOUT DATA BREACH
8
9 --
10
11 Steps to get access on our website:
12
13 1. Download and install tor-browser: https://torproject.org/
14
15 2. Open our website: pb36lu4sp16cyjdfhng7h3pw6dhp32ifemawkujj4gp33ejzdzd3did.onion
16 IF the website is not available, open another one: rnf0sgn6wb6j6su5txekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion
17
18 3. Put your personal code in the input form:
19
20 {
21     "id": "1",
22     "name": "John Doe",
23     "email": "john.doe@example.com",
24     "phone": "1234567890",
25     "password": "1234567890"
26 }
```

Netwalker ransom note for Enel Group

Included in the ransom note, was a link to a <http://prnt.sc/> URL that showed data stolen from the attack. Based on the names of the employees in the folders, it was determined that the attack was on Enel Group.



Screenshot of stolen data shared in ransom note

BleepingComputer emailed Enel Group last week regarding the attack but never heard back.

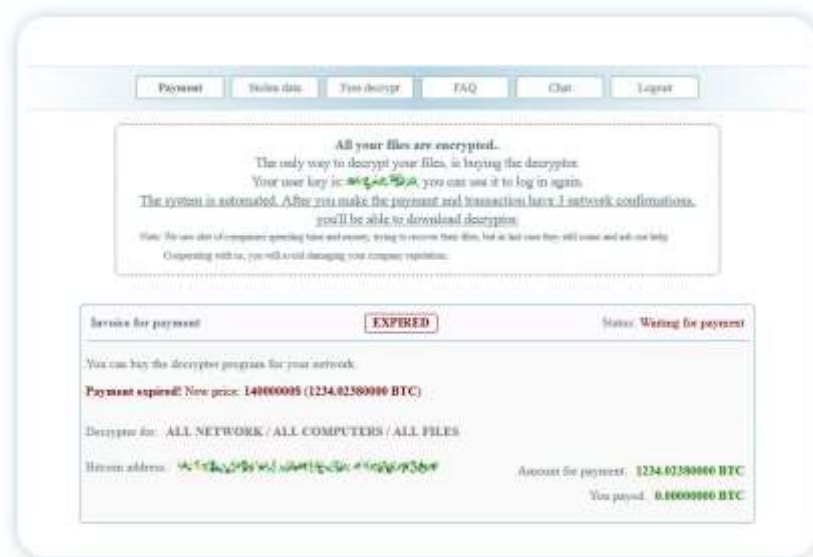
A few days later, Netwalker confirmed that the victim was Enel Group after they added a message to their support chat, stating "Hello Enel. Dont be afraid to write us."



Netwalker chat section for Enel victim page

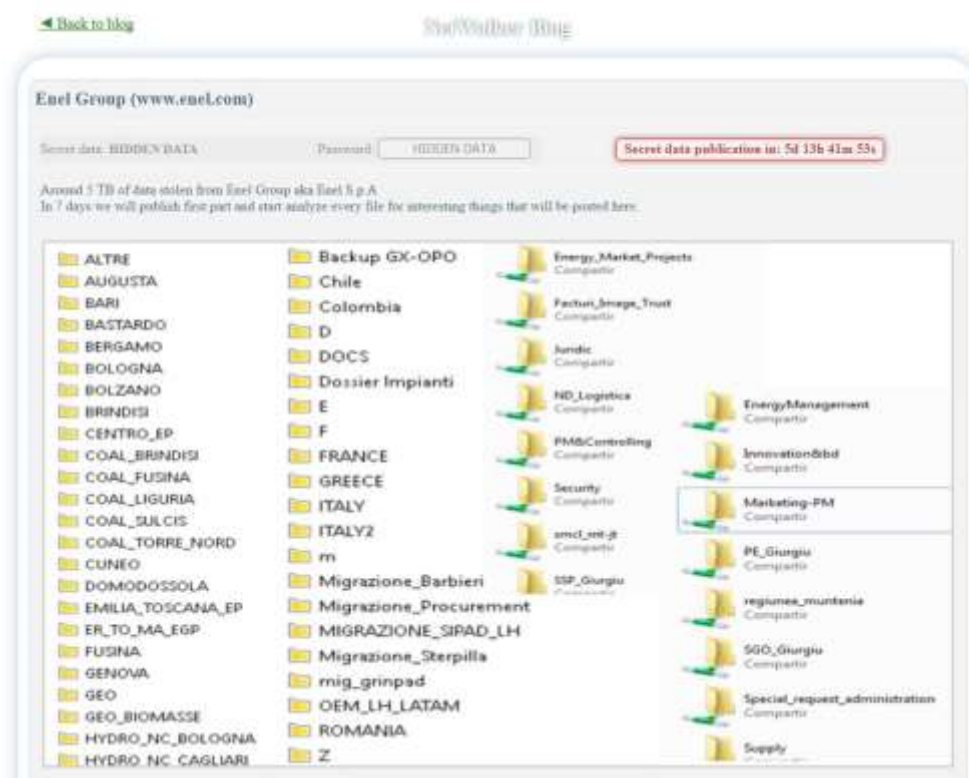
Typically, if the company does not engage the ransom operator in any way, the ransom doubles after a while. It appears that this is what happened with Enel, too, as the private chat provided by the attacker has no conversation from the company.

The attacker used this channel to announce that they would initiate the first step towards leaking the stolen data. This means publishing proof that they have the goods, an attempt to pressure the company into paying the ransom, which is now \$14 million (1234.02380000 BTC).



\$14,000,000 million ransom demand

Today, the Netwalker ransomware gang added Enel Group to their data leak site and shared screenshots of unencrypted files from the company during this month's cyberattack.



According to Netwalker, they stole about 5 terabytes of data from Enel and are ready to make public a piece of it in a week. They also said they would "analyze every file for interesting things" and publish it on their leak site.

This tactic is meant to add pressure and force payment from the victim company. In many cases, this works to the advantage of the attacker.

Source: <https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million/>

14. Maze ransomware is shutting down its cybercrime operation

The Maze cybercrime gang is shutting down its operations after rising to become one of the most prominent players performing ransomware attacks.

The Maze ransomware began operating in May 2019 but became more active in November.

That's when the media-savvy operation revolutionized ransomware attacks by introducing a double-extortion tactic.

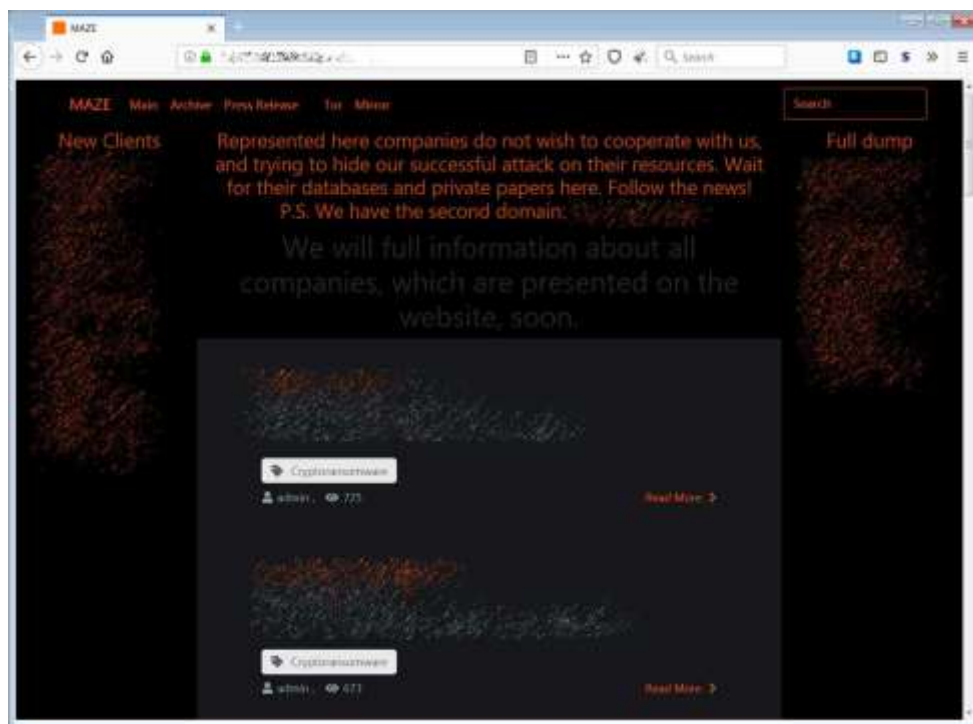
First, they steal your files, then encrypt them

While ransomware operations have always enjoyed [taunting news sites and researchers](#), for the most part, they tended to ignore journalists' emails.

This changed in November 2019, when Maze contacted BleepingComputer to let us know that they [stole the unencrypted data for Allied Universal](#) before encrypting them.

Maze stated that if Allied didn't pay a ransom, their data would be publicly released. Ultimately, the ransom was not paid, and Maze released the stolen data.

Soon after, Maze launched a 'Maze News' site that they use to publish non-paying victims' data and issue "press releases" for journalists who follow their activities.



Maze data leak site

This double-extortion technique was quickly adopted by other large ransomware operations, including REvil, Clop, DoppelPaymer, who released their own [data leak sites](#). This double-extortion technique has now become a standard tactic used by almost all ransomware operations.

Maze continued to evolve ransomware operations by [forming a ransomware cartel](#) with Ragnar Locker and LockBit, to share information and tactics.

During their year and a half cybercrime spree, Maze has been responsible for attacks on notable victims, including [Southwire](#), [City of Pensacola](#), [Canon](#), [LG Electronics](#), [Xerox](#), and many more.

Maze started to shut down six weeks ago

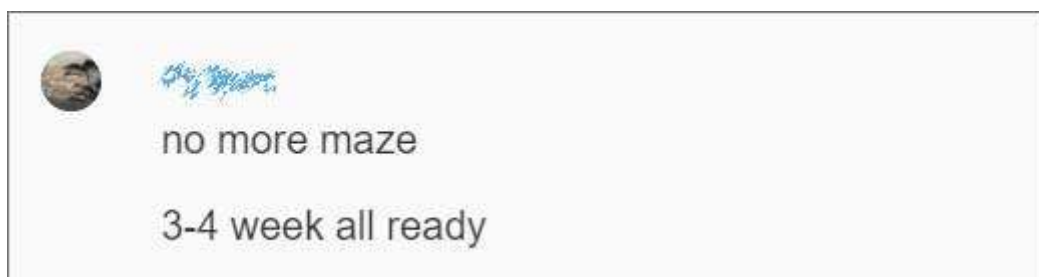
Early last month, BleepingComputer began hearing rumors that Maze was getting ready to shut down their ransomware operation in a similar manner as [GandCrab did in 2019](#).

The closing of operations was later confirmed after BleepingComputer was contacted by a threat actor involved in the [Barnes and Noble ransomware attack](#).

This threat actor stated that they take part in ransomware attacks by compromising networks and stealing Windows domain credentials. The compromised networks are then passed to affiliates who deploy the ransomware.

The group compromising networks, the affiliate, and ransomware developers then take equal shares of any ransom payments.

As part of our conversation, BleepingComputer was told that Maze was in the process of shutting down its operation, had stopped encrypting new victims in September 2020, and are trying to squeeze the last ransom payments from victims.



BleepingComputer told that Maze is shut down

When BleepingComputer reached out to Maze to confirm if they were shutting down, we were told, "You should wait for the press release."

This week, Maze has started to remove victims that they had listed on their data leak site. All that is left on the site are two victims and those who previously had all of their data published.

The cleaning up of the data leak site indicates that the ransomware operation's shutdown is imminent.

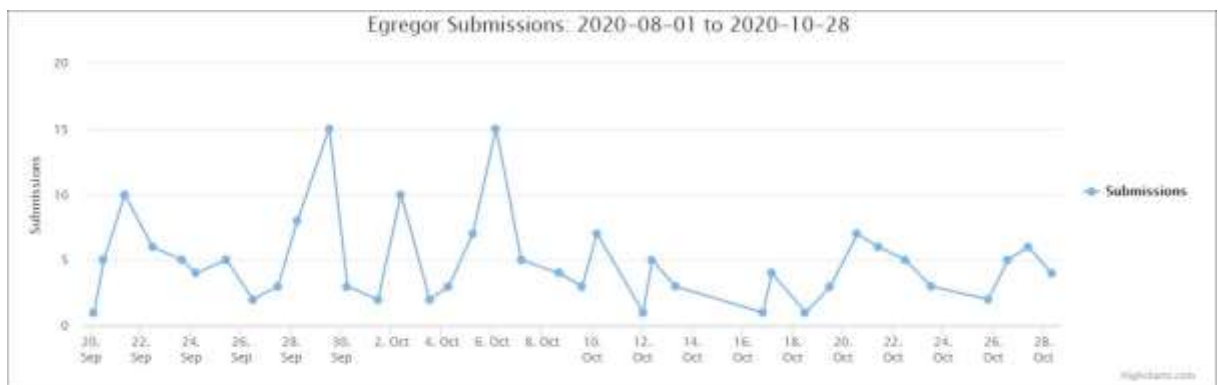
It is not uncommon for ransomware operations to release the master decryption keys when they shut down their operation, as was done with [Crysis](#), [TeslaCrypt](#), and [Shade](#).

BleepingComputer has reached out to Maze to ask if they will release their keys when they shut down their operation but have not heard back.

Affiliates move to Egregor ransomware

BleepingComputer has learned that many Maze affiliates have switched over to a new ransomware operation called Egregor.

Egregor began operating in the middle of September, just as Maze started shutting down their encryption operation. It quickly became very active, as seen by the [ID-Ransomware](#) submission graph below.



Egregor submissions graph to ID-Ransomware

Egregor is believed to be the same underlying software as both Maze and Sekhmet as they utilize the same ransom notes, similar payment site naming, and share much of the same code.

This was also confirmed by a ransomware threat actor who stated that Maze, Sekhmet, and Egregor were the same software.

Ransomware expert [Michael Gillespie](#), who analyzed both Egregor and Sekhmet, also found that Egregor victims who paid a ransom were sent decryptors that were titled 'Sekhmet Decryptor.'



Egregor decryptor

Unfortunately, this shows that even when a ransomware operation shuts down, it does not mean the threat actors involved retire as well. They just move to the next ransomware operation.

Source: <https://www.bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/>

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.