telelink
BUSINESS SERVICES

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

Monthly Security Bulletin

June 2021

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

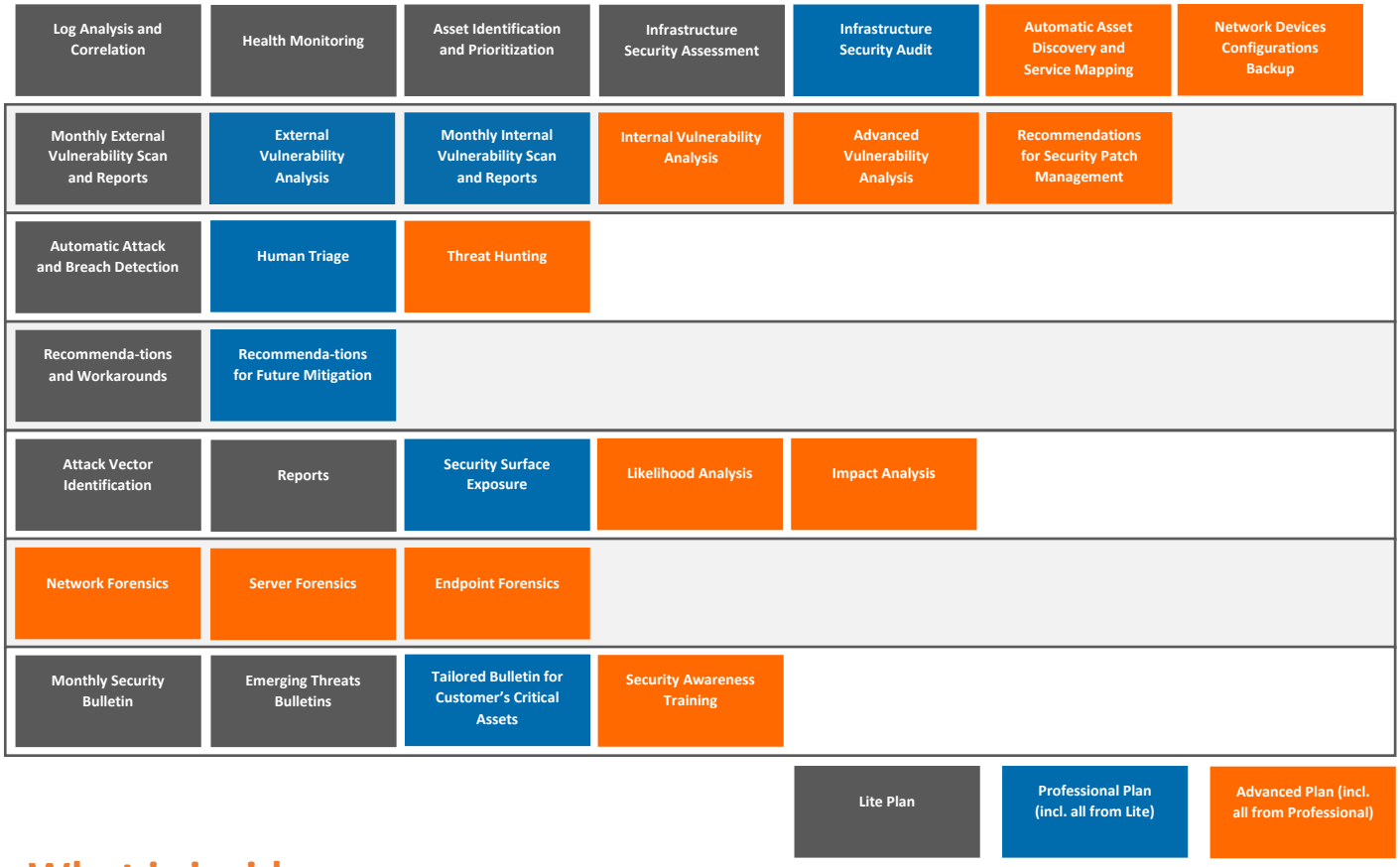
Start to mitigate cyber threats and minimize the risk!

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!



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. Worldwide phishing attacks deliver three new malware strains

A global-scale phishing campaign targeted worldwide organizations across a large array of industries with never-before-seen malware strains delivered via specially-tailored lures. The attacks hit at least 50 orgs from a wide variety of industries in two waves, on December 2nd and between December 11th and 18th, according to a Mandiant report published today. UNC2529, as Mandiant threat researchers track the "uncategorized" threat group behind this campaign, has deployed three new malware strains onto the targets' computers using custom phishing lures.

From downloader to backdoor

The malware used by UNC2529 in these attacks is heavily obfuscated to hinder analysis, and it attempts to evade detection by deploying payload in-memory whenever possible.

"The threat actor made extensive use of obfuscation and fileless malware to complicate detection to deliver a well coded and extensible backdoor," Mandiant said.

Throughout the two waves of attacks, the threat group used phishing emails with links to a JavaScript-based downloader (dubbed DOUBLEDRAG) or an Excel document with an embedded macro that downloaded an in-memory PowerShell-based dropper (known as DOUBLEDROP) from attackers' command-and-control (C2) servers.

The DOUBLEDROP dropper bundles 32 and 64-bit instances of a backdoor (named DOUBLEBACK) implemented as a PE dynamic library.

The backdoor gets injected into the PowerShell process spawned by the dropper. Still, it is designed to later attempt to inject itself into a newly spawned Windows Installer (msiexec.exe) process if Bitdefender's antivirus engine is not running on the compromised computer.

In the next stage, the DOUBLEBACK backdoor loads its plugin and reaches out to the C2 server in a loop to fetch commands to execute on the infected device.

"One interesting fact about the whole ecosystem is that only the downloader exists in the file system," Mandiant added.

"The rest of the components are serialized in the registry database, which makes their detection somewhat harder, especially by file-based antivirus engines."

Signs of spear phishing

UNC2529 used considerable infrastructure to pull off their attacks, with roughly 50 domains being used to deliver the phishing emails.

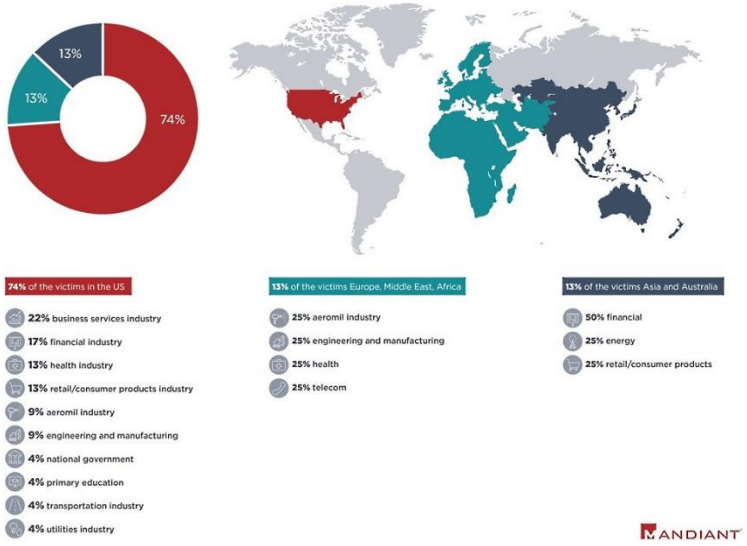
The group also invested time into tailoring their attacks to the targeted victims, in evident attempts to make sure that their emails were seen as legitimate messages from business partners or clients.

They used this tactic to increase the chance that their booby-trapped messages were opened and the targets got infected.

"Masquerading as the account executive, seven phishing emails were observed targeting the medical industry, high-tech electronics, automotive and military equipment manufacturers, and a cleared defense contractor with subject lines very specific to the products of the California-based electronics manufacturing company," according to Mandiant.

UNC2529's phishing campaign was not focused on a single industry vertical or a single region during the two waves of attacks.

While the threat group's primary target area was the US, the attacks also targeted organizations from EMEA (Europe, the Middle East, and Africa), Asia, and Australia.



Although Mandiant has no evidence about the objectives of this threat actor, their broad targeting across industries and geographies is consistent with a targeting calculus most commonly seen among financially motivated groups," Mandiant concluded.

"DOUBLEBACK appears to be an ongoing work in progress and Mandiant anticipates further actions by UNC2529 to compromise victims across all industries worldwide."

Indicators of compromise, including malware hashes and domains used to deliver the phishing emails, are available at the end of Mandiant's report.

Source: https://www.bleepingcomputer.com/news/security/worldwide-phishing-attacks-deliver-three-new-malware-strains/

2. GitHub Prepares to Move Beyond Passwords

GitHub adds support for FIDO2 security keys for Git over SSH to fend off account hijacking and further its plan to stick a fork in the security bane of passwords.

GitHub, the ubiquitous host for software development and version control (and unfortunate target of a steady pitter-patter of attacks targeting the same), is now supporting security keys when using Git over SSH.

In a post on Monday, GitHub security engineer Kevin Jones said that this is the next step when it comes to increasing security and usability. These portable FIDO2 fobs are used for SSH authentication to secure Git operations and to forestall the misery that unfurls when private keys accidentally get lost or pilfered, or when malware tries to initiate requests without user approval. Just one example: In 2019, the TrickBot info-stealing malware got a makeover that enabled its password grabber to target data from OpenSSH applications.

These security keys, which include YubiKey, Thetis Fido U2F Security Key and Google Titan Security Keys, are easy to pop into your pocket and cart around between machines, with most connecting via USB, NFC or Bluetooth. They provide an alternative to the one-time passwords provided by applications or sent via SMS. As it is, SMS SSH codes sent via text can be and have been intercepted.

In contrast, as Jones pointed out, much of the data on a security key is protected from external access and modification, meaning that the key keeps its secrets tucked away and out of reach. While the devices store a private key on your computer, those on-computer keys are simply a reference to the physical security key: in other words, they're useless to anybody who doesn't have the actual device in hand.

Given that the keys are one of the factors in multi-factor authentication (MFA), users should safeguard the devices just like they would any other credential. If you're the only one who can get at your security key, you can, in fact, leave it plugged in. "When using SSH with a security key, none of the sensitive information ever leaves the physical security key device," Jones added. "If you're the only person with physical access to your security key, it's safe to leave plugged in at all times."

Neither malware nor accidental private-key exposure can give away your credentials when you use a security key, he said: "As long as you retain access to the security key, you can be confident that it can't be used by anyone else for any other purpose."

Existing Security Keys Can Still Be Used for Git

"Once generated, you add these new keys to your account just like any other SSH key," Jones said. "You'll still create a public- and private-key pair, but secret bits are generated

and stored in the security key, with the public part stored on your machine like any other SSH public key."

A security key requires you to perform a gesture such as tapping in order to let it know you're about to use the device to authenticate: an action that indicates "user presence," he said, adding that users can also utilize the same security key for both web and SSH authentication, given that they're not limited to a single application. As well, using a security key means that users don't need to use 2FA when authenticating to Git as you would with web authentication.

Users can also check all those authentication boxes, Jones said: "As always, we recommend using a strong password, enrolling in two-factor authentication and setting up account recovery mechanisms." For example, it's possible to use a security key as a recovery option for securely retaining access to a 2FA-enabled account if someone loses access to the phone and backup codes.

(Almost) the Same SSH Keys You Already Love

Not much is changing in terms of how SSH security keys get generated and used. Users can still password-protect their key and require a security key. GitHub data indicates that users likely use an RSA or ed25519 key. Now they have the option of using two additional key types: ecdsa-sk and ed25519-sk, where the "sk" suffix is short for "security key."

GitHub's documentation leads users through creating a new key and adding it to their accounts: A series of steps that's somewhat similar to how it's been done up until now. If someone's ambitious, they can remove previously registered SSH keys and just stick to the SSH keys created by the security keys. That ensures that a user is the only person pulling Git data via SSH, Jones said … as long as the person keeps that security key good and safe.

Stick a Fork in Passwords: They're Done

In its post, GitHub also underscored the fact that it's time to say buh-bye to passwords, the teeth-gnashing security weak spot that humans can't seem to get right. Indeed, two and a half years ago, it seemed like pursuing a password-less future was a road to nowhere.

Even so, in December, GitHub said that it would kill passwords as a way to authenticate Git operations, starting a few months from now, on Aug. 13. The preceding two weeks will be used as a test period in this brave new world of no-passwords-please, where token-based authentication will be required for all authenticated API operations on GitHub.com.

In Monday's post, Jones reiterated that passwords will no longer be supported for Git operations starting later this year, as GitHub continues to embrace more secure authentication patterns.

Don't expect a lot of lemmings to follow GitHub in its war against passwords, said Chester Wisniewski, Principal Research Scientist for Sophos. After all, GitHub users are a cut above when it comes to being technically savvy. "GitHub embracing the death of the password is a great thing but is not likely much of a sign others will follow," he told Threatpost on Tuesday via email. "Because of the nature of GitHub's user base, they are somewhat unique in being able to push forward as their users are technical enough to not be too confused about how tokens and keys work. I suspect it will be harder for them than they expect, as those same technical users will push back with myriad bogus reasons. They don't want to use more secure access methods."

Source: https://threatpost.com/github-security-keys-passwords/166054/

3. Microsoft releases SimuLand, a test lab for simulated cyberattacks

Microsoft has released SimuLand, an open-source lab environment to help test and improve Microsoft 365 Defender, Azure Defender, and Azure Sentinel defenses against real attack scenarios.

SimuLand test labs "provide use cases from a variety of data sources including telemetry from Microsoft 365 Defender security products, Azure Defender, and other integrated data sources through Azure Sentinel data connectors," MSTIC Threat Researcher Roberto Rodriguez said.

Lab environments deployed using SimuLab can help security experts "actively test and verify the effectiveness of related Microsoft 365 Defender, Azure Defender, and Azure Sentinel detections, and extend threat research using telemetry and forensic artifacts generated after each simulation exercise."

SimuLab test environments are designed to help security teams:

- Understand the underlying behavior and functionality of adversary tradecraft.

- Identify mitigations and attacker paths by documenting preconditions for each attacker action.

- Expedite the design and deployment of threat research lab environments.

- Stay up to date with the latest techniques and tools used by real threat actors.

- Identify, document, and share relevant data sources to model and detect adversary actions.

- Validate and tune detection capabilities.

Currently, the only lab environment available for deployment allows researchers to test and improve their defenses against Golden SAML attacks that allow threat actors to forge authentication to cloud apps.

You can share your own end-to-end simulation scenarios by opening new issues on the SimuLand GitHub repository.

Besides working on adding more scenarios, Microsoft also wants to add automation of attack actions via Azure Functions in the cloud, telemetry export and share, Microsoft Defender evaluation labs integration, as well as infrastructure deployment and maintenance using CI/CD pipelines with Azure DevOps.

Lab environments contributed through this open-source Microsoft initiative require an Azure tenant and at least a Microsoft 365 E5 license (paid or trial).

Last month, the Microsoft 365 Defender Research team also released an open-source cyberattack simulator dubbed CyberBattleSim.

This simulator allows creating simulated network environments that model how AI-controlled cyber agents (the threat actors) spread through a network after its initial compromise.

"The simulated attacker's goal is to take ownership of some portion of the network by exploiting these planted vulnerabilities," Microsoft explained.

"While the simulated attacker moves through the network, a defender agent watches the network activity to detect the presence of the attacker and contain the attack."

Source: https://www.bleepingcomputer.com/news/security/microsoft-releases-simuland-a-test-lab-for-simulated-cyberattacks/

4. Comcast now blocks BGP hijacking attacks and route leaks with RPKI

Comcast, one of America's largest broadband providers, has now deployed RPKI on its network to defend against BGP route hijacks and leaks. Left unchecked, a BGP route hijack or leak can cause a drastic surge in internet traffic that now gets misdirected or stuck, leading to global congestion and a Denial of Service (DoS).

Comcast rolls out RPKI to protect BGP routes

This week, in a move to strengthen the security and robustness of its network, telecom giant Comcast has deployed Resource Public Key Infrastructure (RPKI) on its network.

RPKI is a framework designed to secure the Internet's routing infrastructure, primarily Border Gateway Protocol (BGP).

Last month, BleepingComputer reported that a major BGP leak had disrupted thousands of networks globally.

Some of Comcast's prefixes were also present in those advertised by Vodafone's network that suffered the leak.

Vodafone AS55410 - Hijack - 16 April 2021 : VF Hijack		
701	23.29.96.0	UUNET, US
7015	104.143.8.0	COMCAST-7015, US
7015	107.0.159.0	COMCAST-7015, US
7015	107.0.22.0	COMCAST-7015, US
7015	107.0.6.0	COMCAST-7015, US
7015	131.239.42.0	COMCAST-7015, US
7015	137.134.1.0	COMCAST-7015, US
7015	139.181.8.0	COMCAST-7015, US
7015	142.131.200.0	COMCAST-7015, US
7015	149.117.64.0	COMCAST-7015, US
7015	156.96.146.0	COMCAST-7015, US
7015	159.157.206.0	COMCAST-7015, US
7015	159.157.210.0	COMCAST-7015, US
7015	159.215.64.0	COMCAST-7015, US
7015	162.223.144.0	COMCAST-7015, US
7015	164.90.10.0	COMCAST-7015, US
7015	192.149.9.0	COMCAST-7015, US
7015	192.41.172.0	COMCAST-7015, US
7015	192.42.95.0	COMCAST-7015, US
7015	192.88.199.0	COMCAST-7015, US

But, with Comcast's introduction of RPKI to its network, it sounds like the ISP has taken a step forward:

"In practical terms, it means that Comcast now both cryptographically signs route information and validates the cryptographic signatures of other networks' route information."

"This helps to ensure that packets get to their intended destinations intact and cannot be hijacked or leaked to other destinations, making the network – and Internet traffic more generally – more secure and resilient for all users," says Jason Livingood, Vice President of Technology Policy & Standards at Comcast Cable.

"Given the size and technical diversity of our network, deploying RPKI represented a significant effort, yet we were able to implement the update without disrupting performance for our customers," continued Livingood in a blog post this week.

What are BGP, BGP hijacking, and BGP leaks?

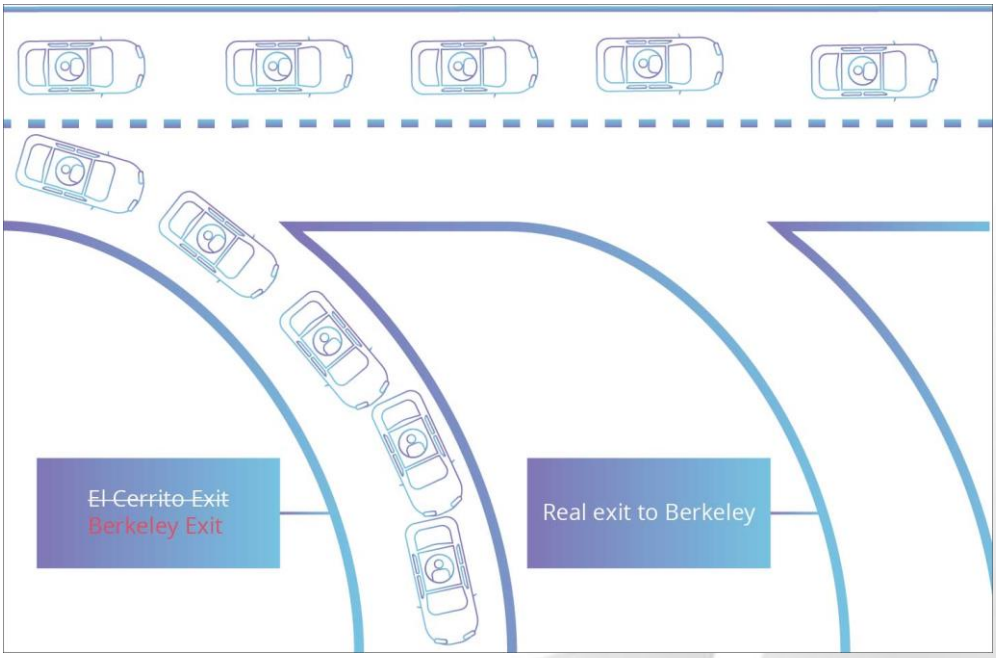
BGP or Border Gateway Protocol is what makes the modern-day internet work.

It is akin to having a "postal system" for the internet that facilitates the redirection of traffic from one (autonomous) system of networks to another.

The internet is a network of networks, and for example, a user based in one country wanted to access a website based in another, there has got to be a system in place that knows what paths to take when redirecting the user across multiple networked systems.

This is similar to a letter being transited through multiple postal branches between its source and destination.

And, that is the purpose of BGP: to direct internet traffic correctly over various paths and systems between the source and destination to make the internet function.



But, BGP is fragile, and any disruptions or anomalies in even a few intermediary systems can have a lasting impact on many.

For the Internet to work, different devices (autonomous systems) advertise the IP prefixes they manage and the traffic they are able to route. However, this is largely a trust-based system with the assumption that every device is telling the truth.

Given the massive interconnected nature of the Internet, it is hard to enforce honesty on every single device present on the network.

BGP route hijacking occurs when a malicious entity manages to "falsely advertise" to other routers that they own a specific set of IP addresses when they don't. When this happens, chaos occurs.

This route confusion would create a lot of trouble on the Internet and lead to delays, traffic congestion, or total outages.

But, BGP route leaks are similar to BGP route hijacking, except the latter more specifically refers to instances of malicious activity taking place.

Whereas, route leaks can be, more likely than not, accidental.

In either case of a BGP route leak or BGP hijacking, an Autonomous System (AS) announces that it knows "how" or "where" to direct the traffic meant for certain destinations (ASes) that in actuality it does not know.

This can lead to the user being taken over an internet route that will offer suboptimal performance or outright cause disruptions and potentially serve as a front for eavesdropping or traffic analysis activities, in cases of malicious hijacking.

Countermeasures like RPKI help by adding validation structures in place by using public-key cryptography.

"RPKI allows network operators to digitally encrypt and sign routing advertisements in Border Gateway Protocol (BGP) by using a system of private and public keys."

"Information can be encrypted and signed with a private key and can only be decrypted, or have its signature verified, using the matching public key."

"Digitally signing information provides assurance that routing advertisements seen in the routing system can be verified and are authentic," states APNIC's guide on RPKI.

This helps networks trust the integrity of route information they are receiving and helps in preventing a DoS incident from an incident of BGP route hijacking or leaks.

Check if your ISP is safe against BGP hijacking

About a year ago, Cloudflare had launched a website where internet users could check if their ISP has added protections against BGP hijacking attacks.

Cloudflare shared some insights on the matter with BleepingComputer:

"Cloudflare launched the isBGPSafeYet.com website over a year ago to help consumers identify if their Internet provider has implemented (or is in the process of implementing) RPKI."

"The goal of this site is to raise awareness around the many ISPs who have still not implemented RPKI and are leaving the Internet vulnerable to route leaks and hijacks," Cloudflare CTO John Graham-Cumming told BleepingComputer in an email interview.

"A network has to deploy RPKI Origin Validation to reject invalid routes. Comcast signing their routes means they are less likely to be impacted by a hijack of their IP address."

"Comcast deploying RPKI Origin Validation means their customers are less likely to be impacted by any hijack on the Internet such as the one targeting myetherwallet in 2018," concluded Graham-Cumming in his interview with us.

Source: https://www.bleepingcomputer.com/news/security/comcast-now-blocks-bgp-hijacking-attacks-and-route-leaks-with-rpki/

5. 100M Android Users Hit By Rampant Cloud Leaks

Several mobile apps, some with 10 million downloads, have opened up personal data of users to the public internet – and most aren't fixed.

More than 100 million Android users are at risk after 23 different mobile apps were found to leak personal data in the wake of rampant cloud misconfigurations.

That's according to Check Point Research, whose researchers found that emails, chat messages, location data, passwords, photos, personal data and more were all available to anyone with an internet connection. Worryingly, after being contacted by the firm, only "a few" of the apps have changed their settings to make the information private.

Researchers also found push-notification and cloud-storage keys embedded in a number of Android applications, which put developers' own internal resources, such as access to update mechanisms, storage and more, at risk.

Real-Time Databases Left Open to Snoopers

The data was accessible from real-time databases in 13 of the Android apps, whose download numbers range from 10,000 to 10 million. The apps were for things like astrology, taxi services, logo-makers, screen recording and faxing, researchers said.

Real-time databases allow application developers to store data on the cloud, so that each time an app connects, information is synchronized and the clients (and the databases) are brought up to date. However, for the examined apps, there was no authentication check to access them.

In the case of T'Leva, a taxi app with more than 50,000 downloads, researchers were able to access chat messages between drivers and passengers, plus location data and personal information like full names and phone numbers – all by sending one request to the database.

One of the offending apps, Astro Guru, has more than 10 million downloads. It offers horoscopes, palmistry and similar services. Since it provides personalized "readings," it asks for a lot of information, including name, date of birth, gender, location, emails and, of course, payment details. Once that's completed, Astro Guru delivers a "personal astrology and horoscope prediction report."

This could be weaponized in ingenious ways, such as hackers intercepting news alerts to replace legitimate content with fake news, or phishers injecting phishing links into the notifications – all of which are sent from the legitimate app, so users are none the wiser.

Cloud Keys Up in the Air for the Taking

In the case of at least two of the apps, cloud keys were exposed with no safeguards, according to the researchers.

For instance, the Screen Recorder app does what it says – it records the user's screen and then saves the recordings in the cloud for later access. It has more than 10 million downloads.

Unfortunately, the developers saved users' private passwords on the same cloud service that stores the recordings.

"With a quick analysis of the application file, [Check Point] researchers were able to recover the mentioned keys that grant access to each stored recording," they explained.

It's a bad practice to hardcode and store static access keys into an app, Michael Isbitski, technical evangelist at Salt Security, said via email.

What to Do if Your Data is Leaked by an App

Imperva Research Labs has found that data-leakage incidents have increased 557 percent over the past 12 months, and are up 74 percent since the beginning of 2021, according to Ron Bennatan, general manager for data security for Imperva.

"Enterprises need to stop thinking of application security and data security as disparate entities, because attackers certainly aren't thinking that way, and it's creating opportunities for them to access data," he said. "A good enterprise takes a data-centric approach and secures the data itself, and not just the endpoints connected to the database."

Cloud misconfigurations that leave data publicly exposed happen all the time, in other words – and unfortunately, there's very little that end users can do to protect themselves from an exposure. But there are steps to take after a data leak occurs, researchers said.

"End users can take proactive steps to protect themselves when their data does get exposed," Irene Mo, senior consulting associate at Aleada, said via email. "My two top tips are: 1) set up multifactor authentication for every account that offers it, and 2) lie on account security questions. The answers to common security questions, like a user's childhood street name or their favorite color, can be found publicly online. If a user lies on their security questions, only the user knows how they lied. And to keep track of their lies (a bonus tip), use a password manager."

Source: https://threatpost.com/100m-android-users-cloud-leaks/166372/

6. Building SIEM for Today's Threat Landscape

Sivan Tehila, cybersecurity strategist at Perimeter 81, discusses the elements involved in creating a modern SIEM strategy for remote work and cloud-everything.

It's easy to see how the changing security landscape has shaped the evolution of the security information and event management (SIEM) practice area — and how it continues to. But architecting an effective SIEM approach requires a well-thought-out strategy.

A combination of security information management (SIM) and security event management (SEM), SIEM's development over the last 16 years has been directly tied to different market drivers and threats during any given time period.

Why SIEM is an Ideal Setup, Now More Than Ever

SIEM software uses analytics engines to match events against an organization's policies. Then it indexes the data and events for a sub-second search to detect and analyze advanced threats using globally gathered intelligence.

When SIEM identifies a threat through network-security monitoring, it generates an alert and defines a threat level based on predetermined rules. For example, if someone is trying to log into an account 10 times in 10 minutes, that may be considered normal — but trying to log in 100 times within 10 minutes would be flagged as an attempted attack.

With endpoints now scattered outside the corporate network, cloud adoption on the rise and new applications meeting new needs for remote workers, SIEM has become an even more useful tool, since it gives security teams a centralized view of insights and activities within their IT environment. It provides data analysis, event correlation, aggregation, reporting and log management.

Alert Fatigue is Real

Despite the benefits, not all SIEM solutions are easy to deploy, maintain and manage. Automation is essential to SIEM adoption and ongoing effectiveness.

According to the 2020 State of SecOps and Automation survey, 92 percent of organizations agree that automation is required to address the growing number of alerts, as well as the high volume of false positives.

Still, 65 percent of organizations use only partially automated alert processing, and 75 percent would need no fewer than three additional security analysts to deal with all alerts on the same day.

The Need for Speed Requires Add-Ons

Modern security threats are driving a need for layered analytics with security platforms. AI, machine learning and advanced analysis ca automate the detection of anomalous behaviors and improve response time even more, stopping any potential attacks on the organization in real-time, proactively and reactively.

Beyond using AI and machine learning for better correlations and alerts, most SIEM systems also have a threat-detection element that monitors emails, cloud resources, applications, external threat intelligence sources and endpoints. This can include user and entity behavior analytics (UEBA), which monitors for abnormal behaviors that could indicate a threat. It can also detect behavior anomalies, lateral movement and compromised accounts.

Any capable SIEM solution will always require organizations to manage an increasing number of data sources. Due to the ongoing shortage of cybersecurity skills, it's important to adopt a solution with vendor support in the form of ongoing updates and best practices, so your IT team won't be forced to be SIEM experts.

Along with UEBA, extended detection and response (XDR) or security orchestration, automation and response (SOAR) can help bring the necessary visibility and flexibility a SIEM system requires. SOAR encompasses three software capabilities – threat and vulnerability management, security incident response and security operations automation.

Proper SIEM setup today means you'll be prepared for the next evolution, and whatever challenges that may bring.

Source: https://threatpost.com/building-siem-threat-landscape/166390/

7. 5 Unique Online Scams and How to Defend Against Them

The possibility of an online scam can be an ever-changing problem for individuals and businesses. If someone clicks on a virus-laden email while employed in a data-heavy business, their stolen data could lead to a compromise to the business overall. Because of this, knowing what your employees might encounter in their day to day is also part of internal cybersecurity. Here are five online scam methods that stood out for their innovation and uniqueness in the last year.

Online Scam Methods Amid a Pandemic

The digital threat landscape witnessed a surge of activity in the first half of 2020. In the middle of April, for instance, VMware Carbon Black revealed that global organizations had experienced a 148% spike in ransomware attacks up until that point for the year. Those attacks had affected organizations in every sector, though the financial sector had witnessed the largest increase. Around that same time, Barracuda disclosed that spearphishing campaigns leveraging COVID-19 as a lure had grown 667% between the end of February and March of 2020.

It's not surprising that many of those attack campaigns preyed upon targets' fears surrounding COVID-19. What is surprising is the number of online scam attacks with unique subjects, lures and approaches — regardless of whether they mentioned the pandemic.

Anti-Virus that Defends Against Actual Viruses?

Malwarebytes posted an online scam report about a website offering "Corona Antivirus" in March last year. This digital solution claimed that people could protect themselves against COVID-19 as long as their desktop app was running.

Unsurprisingly, this piece of software didn't yield any cross-medium virus cure. Instead, it infected the victim with BlackNET, a botnet that is capable of stealing its victims' data and running distributed denial-of-service (DDoS) attacks.

Fake Charges for Activating Roku Devices

A couple of months later, the Better Business Bureau learned of an online scam targeting people who had purchased a Roku device. In one instance reported by NBC12 in May that a strange message popped up when a Cincinnati woman attempted to finish setting up her device. This message instructed her to contact a Texas-based company in order to pay an installation fee for her product.

Roku doesn't charge installation fees for its devices.

The woman was ultimately reimbursed for the 'fee' she paid. The Better Business Bureau also gave the company in Texas the opportunity to clarify its role with Roku. When the company didn't respond, the non-profit organization responded by handing out an 'F' rating to the Texas business.

A New Wave of Brushing Scams

In the late spring and summer of 2020, all 50 states issued a warning after residents began receiving mysterious seeds in packages sent from China. The U.S. Department of Agriculture identified that those packages contained seeds for common vegetables such as cabbage and herbs such as sage, reported USA Today. Even so, it urged people not to plant the seeds and to contact their state's plant regulatory authority.

Not long after, USA Today learned of a similar online scam in which individuals were receiving packages from Amazon containing items that they had not purchased. The Better Business Bureau said this "brushing" scam came from fraudsters in the possession of victims' personal information who were likely abusing that data to post fraudulent customer reviews for the purpose of boosting sales.

Beware of Missing Person Ploys

Near the end of summer last year, Malwarebytes sounded the alarm of fraudsters using fake missing person notices for different kinds of malicious purposes. The security firm found that domestic abusers could use these ruses to find someone with whom they had

a history of abuse, for instance. It also observed that nefarious individuals could conduct those scams in order to compromise victims' web accounts.

In one example cited by Malwarebytes, digital fraudsters created a ruse that claimed a child had gone missing. The scam used generic terms such as "police captains" and "downtown" in an attempt to phish victims' data for their Facebook accounts.

Scammers Impersonate the U.S. Department of Justice

A week or so later the U.S. Department of Justice (DOJ) drew attention to a new online scam discovered by the Office of Justice Programs' Office for Victims of Crime.

At the time of reporting, the National Elder Fraud Hotline had received multiple reports of fraudsters contacting elderly people while pretending to be employees or investigators connected with the DOJ. Upon linking with their target, those threat actors attempted to use scare tactics as a means of tricking victims into handing over their personal data.

How to Defend Against Innovative Online Scams and Attacks

The instances described above highlight the need for enterprise and users alike to defend against new online scams and digital attacks. One of the ways they can do this is by enhancing their defenses against phishing attacks. Organizations can do this by using email security filters to flag messages that originate from external sources and by training their employees about some of the latest phishing attacks circulating in the wild. Employees can then apply that knowledge at home in order to keep their home networks and devices safe from malicious actors.

It's also important that enterprise leaders and users take steps to protect themselves on social media. To do this, they should take their privacy into consideration and generally refrain from disclosing their name, location or sensitive information. They should also watch out for offers that sound too good to be true from contacts and/or unfamiliar individuals.

Source: https://securityintelligence.com/articles/five-unique-online-scams

8. VMware Sounds Ransomware Alarm Over Critical Severity Bug

VMware's virtualization management platform, vCenter Server, has a critical severity bug the company is urging customers to patch "as soon as possible".

VMware patched a critical bug impacting its vCenter Server platform with a severity rating of 9.8 out of 10. The company said the flaw could allow a remote attacker to exploit its products and take control of a company's affected system.

VMware went a step further on Tuesday, calling on IT security teams – already on high alert over an uptick in costly and destructive ransomware attacks – to patch systems fast.

Critical Bug Impacts Critical Mass?

The vulnerability, tracked as CVE-2021-21985, impacts vCenter Server platforms, which is in widespread use and used to administer VMware's market leading vSphere and ESXi host products.

Claire Tills, a senior research engineer with Tenable wrote in a post commenting on the bug, "patching these flaws should be a top priority. Successful exploitation would allow an attacker to execute arbitrary commands on the underlying vCenter host."

Tills note exploiting the vulnerability is trivial. All an attacker would need to do is be able to access vCenter Server over port 443, she wrote. "Even if an organization has not exposed vCenter Server externally, attackers can still exploit this flaw once inside a network."

Kenna Security's director of security research Jerry Gamblin, however noted estimates of how many networks are vulnerable attacks is relatively small.

"Some early research from Rapid 7 shows that only around 6K's VCenters are exposed directly to the internet, which makes the 'blast radius' tiny and the initial entry point into a network unlikely with this pair of CVES," Gamblin wrote in an email commentary to Threatpost.

Gamblin is referring to both the critical CVE-2021-21985 bug and a second vulnerability reported by VMware on Tuesday, CVE-2021-21986. This second bug has a medium CVSS severity rating of 6.5 and is tied to an authentication mechanism issue in vCenter Server plugins.

Breaking Down the Critical Bug

Workarounds and updates are available to mitigate both flaws, according to VMware.

"The vSphere Client (HTML5) contains a remote code execution vulnerability due to lack of input validation in the Virtual SAN Health Check plug-in which is enabled by default in vCenter Server," VMware's security bulletin states for the critical (CVE-2021-21985) bug. "The affected Virtual SAN Health Check plug-in is enabled by default in all vCenter Server deployments, whether or not vSAN is being used."

VMware's Virtual San (or vSAN) is a software-defined storage solution that typically supports hyper-converged infrastructure. The Health Check plug-in "checks to monitor the status of cluster components, diagnose issues, and troubleshoot problems," according to a VMware description of the tool.

VMware credited the researcher identified only as "Ricter Z" of 360 Noah Lab for finding the bug.

Source: https://threatpost.com/vmware-ransomware-alarm-critical-bug/166501/

9. The Cybersecurity Ecosystem: How Did It Get So Crowded?

Peek inside any enterprise security operations center (SOC) today, and you'll likely see a crowded and high-pressure cybersecurity ecosystem. Over the past few years, as technology evolved rapidly, attackers have developed a growing array of strategies and tactics. In response, security organizations have deployed more and more tools and point solutions, engaged with increasing numbers of vendors and service providers and collected ballooning volumes of data.

To what end? According to research conducted by Forrester Consulting on behalf of IBM, the average organization's cybersecurity ecosystem now involves 25 disparate security products and services from 13 different vendors, with major enterprises using more than 100 unique security tools.

But as the Ponemon Institute's most recent Cyber Resilient Organization Report reveals, security operations programs using fewer than 50 security solutions are 9% better at detecting attacks and 7% better at defending against attacks than SecOps programs using more than 50 solutions. How did we arrive at this point where more solutions means more problems?

How the Cybersecurity Ecosystem Grew

To answer this question, we'll trace the evolutionary history of today's cybersecurity ecosystem. Throughout the development of networked computing, increasing systems'

connectivity and improving functionality was generally seen as more important than decreasing security risks. Early systems were simply not designed with security in mind. Once discovered, openings in the cybersecurity ecosystem were addressed in a reactive fashion.

Today's IT systems are already far more complex than the first large-scale general-purpose computing networks, of course. And as they swell to include rising numbers of mobile devices, Internet of things (IoT) sensors, cloud services and software-as-a-service (SaaS), they're only getting more complex. As long as enterprises continue to respond to this expansion in a reactive fashion, however, the excesses — too much data, too many alerts, too much code, too many silos and too much work for security teams — will remain.

The Early Era: 1970s – 1980s

The earliest computer viruses and "worms" in the cybersecurity ecosystem were tests rather than malicious in nature. Creeper, widely considered the world's first virus, was developed by researchers exploring how code could travel across networks and replicate itself. The Morris Worm, another early malware program, was intended to gauge the size of the internet. Running the code taxed the resources of the computers it infected, causing many of them to crash — a forerunner to today's distributed denial of service (DDoS) attacks, but on a much smaller scale. The damage that such stunts could cause was limited, since most computers at this time only networked locally, if at all.

The Birth of the Firewall: Early Corporate Networks (1988-1992)

As network connectivity became more popular in enterprise computing and awareness that viruses could damage the cybersecurity ecosystem grew, researchers at Digital Equipment Corporation (DEC) created and ran the first internal corporate firewall in 1988. Their design became the basis for the first commercial firewall, DEC SEAL, which shipped in 1992.

The developers modeled the network firewall after the architectural structures used to prevent fires from spreading across large buildings. Routers separated networks into sub-groups and logged and screened all traffic before allowing it to pass between them. The idea was to ensure an attack affecting one part of the network could no longer compromise the whole. All traffic filtering occurred on the basis of prewritten rules, so firewall designers had to know which sources were likely malicious before they could write these rules — a reactive approach.

Dawn of the Internet: The Antivirus Era (1990s)

In the early 1990s, the National Science Foundation (NSF) lifted all restrictions on commercial use of the Internet. Within a year, and following the introduction of Mosaic, the first multimedia World Wide Web browser, Internet usage began doubling every three

months. Threat actors caught on to the trend right away: as the Internet grew, malware designed to infiltrate corporate networks and consumers' home computers — stealing data and destroying systems along the way — spread rapidly as well.

Early antivirus programs compared signatures (file hashes and, later, code strings) from known malware with files on users' computers to spot infection. Not only was this approach to preventing virus infection reactive by design, but it was research-intensive. Specific features of the malicious code had to be detected before updates could be delivered to an antivirus company's customers.

This approach positioned defenders one step behind attackers, awaiting their next move. In addition, antivirus software tended to have high false positive rates when it came to detecting malware. And, antivirus products were often resource-intensive to run, interfering with user experience or malfunctioning if used in conjunction with other vendors' antivirus tools.

Reacting to a Problem: The Firewall as Single Point of Failure

Firewalls protected only a single entry point into the network. Therefore, they were useless if an intruder found another way into the cybersecurity ecosystem. In response, defenders developed Intrusion Detection Systems (IDS) to look for system changes or streams of packets on a network that were connected with known attacks. Early systems were network-based, meaning they collected and scanned traffic packets to find signs of malicious traffic.

To be effective, IDS required a database of indicators to determine whether traffic was threatening. So, like antivirus software products, these systems depended on prior knowledge of current threats. IDS collected growing amounts of data on the health and status of IT environments, which security analyst teams then monitored and analyzed.

Rise of the SIEM: The Compliance Era

High-profile incidents ranging from the Yahoo! logic bomb to the spread of Microsoft Windows 98 bugs attracted increasing amounts of public scrutiny. Governments began to require companies to follow better cybersecurity practices. Enterprises encountered new legal mandates to collect and maintain network log data for audits.

Where could security teams store all this data so that they could retrieve it for use in incident investigations? How could they make it easy to understand? To solve these problems, security information management (SIM) tools came into widespread use. By this stage, most SOCs used an assortment of security tools in their cybersecurity ecosystem, often from multiple vendors. Teams needed a centralized system that could automate the collection of log data from firewalls, antivirus software and other sources of endpoint and network telemetry data. They also needed a way to translate the raw log data into common formats that were simpler to search and report on.

But searching the cybersecurity ecosystem for large volumes of log data was complex, lengthy and usually only performed in the aftermath of a known incident. To make it possible for teams to detect in-progress attacks, vendors expanded SIM tools into system information and event management (SIEM).

The event management component of this technology involves spotting red flag activities. Analysts create rules or algorithms to do this that reflect the specifics of their networks. The adoption of SIEM technologies meant that security operations teams were now responsible for more programming — and handling still more data — than they had been in the past.

Cloud Computing Makes the Cybersecurity Ecosystem More Complex

Amazon Web Services (AWS) launched in 2006. By the late 2000s, public cloud computing's worldwide rise had blossomed as providers made previously unheard-of computing power available on a subscription basis. The benefits of cloud computing are legion, but it also has drawbacks. It makes the cybersecurity ecosystem much more complex and dissolves walls between networks.

Security organizations have continued to add point solutions to address challenges that cloud computing has brought, often adding separate teams to manage these new tools. In many cases, they brought in solutions for different endpoints, hardware, and tools side-by-side. The task of merging the data, policy and management of these behemoth security architectures is not easy.

Future Cybersecurity Ecosystem Challenges

Things won't get simpler in the near future. IoT adoption will increase the number of connected devices. At the same time, 5G networking will speed up demand for mobile devices to access corporate computing resources. Meanwhile, 'big data' and newly powerful analytics dependent upon quantum computing will exponentially increase the number of operations that can be performed in any given time frame.

The challenges remain. Teams will continue to struggle to maximize the value of the tools they already have in place in their cybersecurity ecosystem. This solution is to put systems in place that will allow those tools to freely exchange data. This, in turn, can power analytics and support automated incident response workflows. What's needed is an open ecosystem where cybersecurity products can work together without the need for customized connectors. In this world, vendors, end users and cybersecurity researchers can meet to develop code, standards and practices that security operations teams can share over the entire threat management life cycle.

This vision of the future is already here. In the Open Cybersecurity Alliance project, a number of the world's leading cybersecurity organizations have come together in support

of seamless interoperability. The focus of the project is to make data interchange easier within security operations. It's chasing the dream of making sure cybersecurity tools can work together simply and effectively.

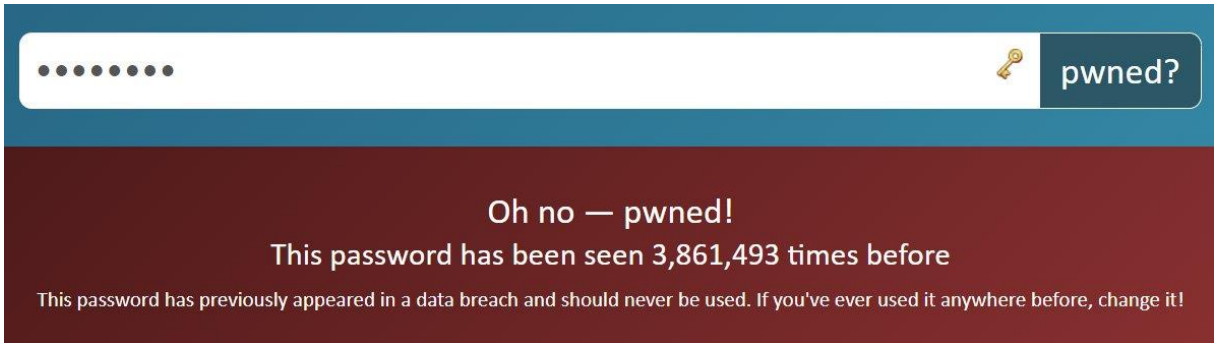
Source: *https://securityintelligence.com/articles/cybersecurity-ecosystem-how-did-it-get-so-crowded*

10. FBI to share compromised passwords with Have I Been Pwned

The FBI will soon begin to share compromised passwords with Have I Been Pwned's 'Password Pwned' service that were discovered during law enforcement investigations.

The Have I Been Pwned data breach notification site includes a service called Pwned Passwords that allows users to search for known compromised passwords.

Using this service, a visitor can input a password and see how many times that password has been found in a breach. For example, if we enter the password 'password,' the service states that it has been seen 3,861,493 times in data breaches.



Password Pwned search for 'password'

Today, Have I Been Pwned creator Troy Hunt announced that the FBI would soon be feeding compromised passwords found during law enforcement investigations into the Pwned Password service.

By providing this feed, the FBI will allow administrators and users to check for passwords that are known to be used for malicious purposes. Admins can then change the passwords before they are used in credential stuffing attacks and network breaches.

The FBI will share the passwords as SHA-1 and NTLM hash pairs that can then be searched using the service or downloaded as part of Pwned Password's offline list of passwords.

Password Pwned allows users to download the compromised passwords as lists of SHA-1 or NTLM hashed passwords that can be used offline by Windows administrators to check if they are being used on their network.

To help facilitate this new partnership, Hunt has made Password Pwned open source via the .NET Foundation and is asking other developers to help create a 'Password Ingestion' API.

The FBI and other law enforcement agencies can use this API to feed compromised passwords into the Password Pwned database.

Source: https://www.bleepingcomputer.com/news/security/fbi-to-share-compromised-passwords-with-have-i-been-pwned/

11. Hackers Exploit Post-COVID Return to Offices

Spoofed CIO 'pandemic guideline' emails being used to steal credentials.

With COVID-19 restrictions lifting and workers trickling back to offices, threat actors are sharpening their spear phishing ploys. The latest scam includes pelting recipients with emails purportedly from their CIOs welcoming employees back into offices.

The emails outline a company's post-pandemic cubicle protocols, at the same time attempt to steal company and personal credentials.

"The body of the email appears to have been sent from a source within the company, giving the company's logo in the header, as well as being signed spoofing the CIO," Cofense outlined in a Thursday report.

The fake newsletter explains return-to-work procedures are forcing employees to take new precautions relative to the pandemic, according to the researchers.

COVID Scam Targets Credentials

The spoofed CIO email prompts victims to link to a fake Microsoft SharePoint page with two company-branded documents, both outlining new business operations. In this step the victim is not prompted to input any credentials.

"Instead of simply redirecting [victims] to a login page, this additional step adds more depth to the attack and gives the impression that they are actual documents from within the company," according to the report.

However, if a victim decides to interact (click) on either document a login panel appears and prompts the recipient to provide login credentials to access the files.

Exploitation of COVID-19

With over half of U.S. adults now having received at least one vaccine shot, more employees are going back to work. HR consultancy Mercer reports 61 percent of enterprise employers hope to have half or more of their workforce back in the office by the end of the third quarter of 2021. Bellwether firms Microsoft and Google, for example, have already begun a measured process of repopulating their office cubicles with on premise staff.

This certainly isn't the first time attackers have used COVID-19 to their advantage.

Vaccine-related spear phishing attacks spiked 26 percent between Oct. 2020 and January 2021, just as the life-saving drugs were being rolled out. Healthcare organizations and hospitals have been specifically targeted as they've been crushed under the weight of the pandemic. Between Jan. 2020 and Sept. 2020 10 percent of all organizations targeted by ransomware were hospitals or medical organizations.

Just last month, as governments rolled out pandemic relief payments, attackers used fake U.S. aid payments to deliver Dridex Malware.

"COVID-19 has given us a window into how hackers can exploit human vulnerabilities during a crisis, with healthcare and pandemic-related attacks prevalent in 2020," Sivan Tehila with Perimeter 81 wrote recently for Threatpost.

Cybercriminals thrive on change and only become emboldened by it, rolling out new cybercrime offenses to exploit trending news events, she said.

Source: https://threatpost.com/hackers-exploit-covid-office/166550/

12. Watch out: These unsubscribe emails only lead to further spam

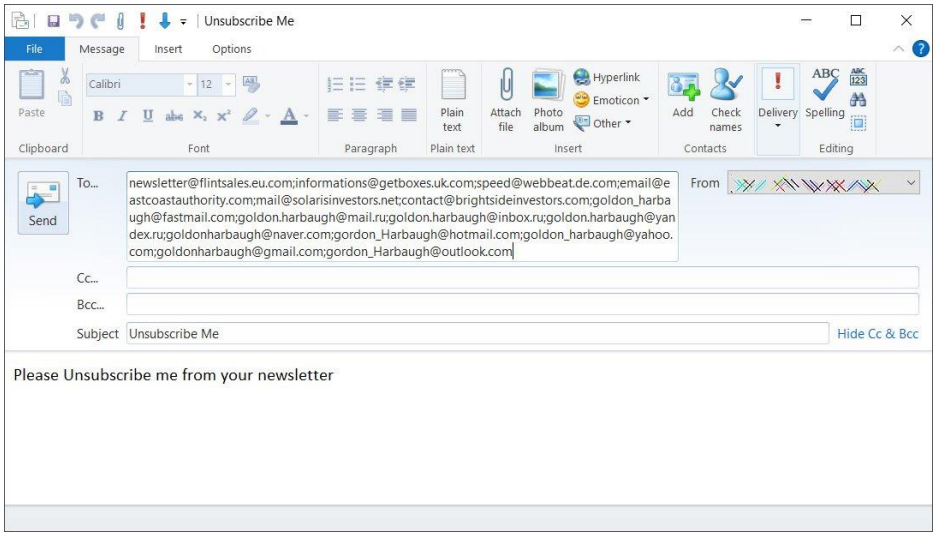
Scammers use fake 'unsubscribe' spam emails to confirm valid email accounts to be used in future phishing and spam campaigns.

For some time, spammers have been sending emails that simply ask if you wish to unsubscribe or subscribe. These emails do not explain what you are unsubscribing or subscribing to and are being used by spammers to verify if the recipient's email is valid and susceptible to phishing scams and other malicious activity.

The "confirmation" emails use mail subjects, such as "We_need your confirmation asap", "Request , please confirm your unsubscription", and "Verification."

The email messages are very basic, with just colorful boxes containing links asking whether you would like to unsubscribe or subscribe, as shown below.

If you click on the embedded subscribe/unsubscribe links, it will cause your mail client to create a new email that will be sent to many different email addresses under the spammer's control.



When users send the above email, they expect to be unsubscribed from further emails. However, they are actually verifying for the spammers that their email address is valid and being monitored.

Responding leads to more spam

As a test, BleepingComputer created a new email address that we never used on any website or service. Using this email address, we responded to various confirmation emails that we received on another email account.

After sending unsubscribe/subscribe responses from the new account, in only a few days our new account became bombarded with spam emails.

This test further confirmed that spammers are using these subscribe/unsubscribe emails to refine their mailing lists and verify email addresses susceptible to these types of scams and phishing attacks.

If you receive an email that just simply asks you to subscribe or unsubscribe, ignore it and mark it as spam.

No legitimate organization will send these types of emails without further explaining what the email is referencing.

Source: https://www.bleepingcomputer.com/news/security/watch-out-these-unsubscribe-emails-only-lead-to-further-spam/

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.