telelink
BUSINESS SERVICES

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

Monthly Security Bulletin

October 2021

This security bulletin is powered by Telelink Business Services'

Advanced Security Operations Center

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

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

The ASOC by Telelink Business Services 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 Business Services?

- 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

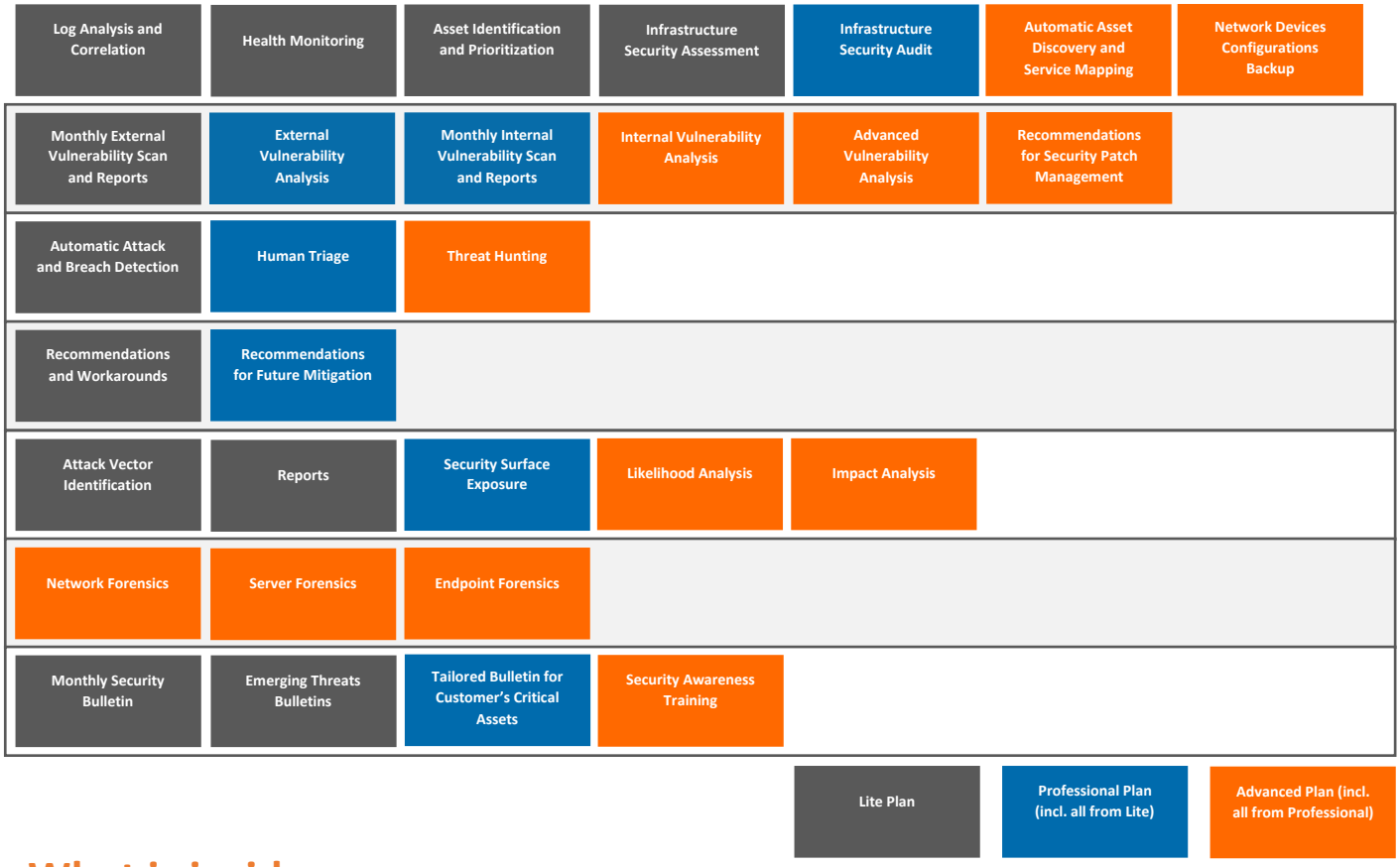
Start to mitigate cyber threats and minimize the risk!

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. Over 60,000 parked domains were vulnerable to AWS hijacking 4
2. Hackers leak passwords for 500,000 Fortinet VPN accounts 9
3. Microsoft rolls out passwordless login for all Microsoft accounts 13
4. No Patch for High-Severity Bug in Legacy IBM System X Servers 14
5. Billions more Android devices will reset risky app permissions 16
6. TangleBot Malware Reaches Deep into Android Device Functions 17
7. Exchange/Outlook Autodiscover Bug Spills 100K+ Email Passwords 19
8. Microsoft will disable Basic Auth in Exchange Online in October 2022 25
9. 5 Steps to Securing Your Network Perimeter 26
10. Working exploit released for VMware vCenter CVE-2021-22005 bug 30
11. Threat Actors Weaponize Telegram Bots to Compromise PayPal Accounts 32
12. GriftHorse Money-Stealing Trojan Takes 10M Android Users for a Ride 34
13. Facebook open-sources tool to find Android app security flaws 37
14. Google pushes emergency Chrome update to fix two zero-days 39

1. Over 60,000 parked domains were vulnerable to AWS hijacking

Domain registrar MarkMonitor had left more than 60,000 parked domains vulnerable to domain hijacking.

MarkMonitor, now part of Clarivate, is a domain management company that "helps establish and protect the online presence of the world's leading brands - and the billions who use them."

The parked domains were seen pointing to nonexistent Amazon S3 bucket addresses, hinting that there existed a domain takeover weakness.

Researchers took over 800 root domains

This week, security engineer and bug bounty hunter Ian Carroll saw his automation script flag hundreds of domains belonging to different organizations that were vulnerable to domain hijacking.

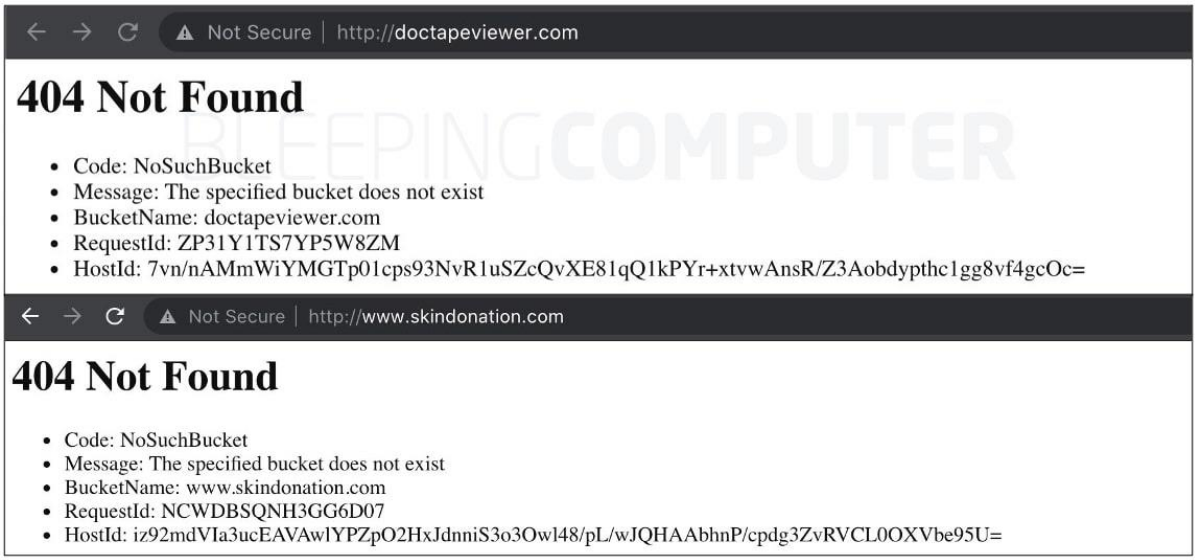
Carroll was then joined by Nagli and *d0xing* who helped the engineer trace the source of the security weakness. All of the domains shared the same registrar—MarkMonitor.

(Sub)domain takeover refers to an unauthorized actor being able to serve the content of their choice on a domain they otherwise have no rights to or ownership of.

This can occur, for example, if the domain name has a canonical name (CNAME) DNS entry pointing to a host that is not providing any content for it.

Typically, this happens if the website hasn't been published yet or the virtual host has been removed from a hosting provider but the domain's DNS records continue to point to the host.

When such a scenario occurs, what follows is a 404 (not found) error message when one attempts to access the domain, indicating that a domain takeover weakness could exist.



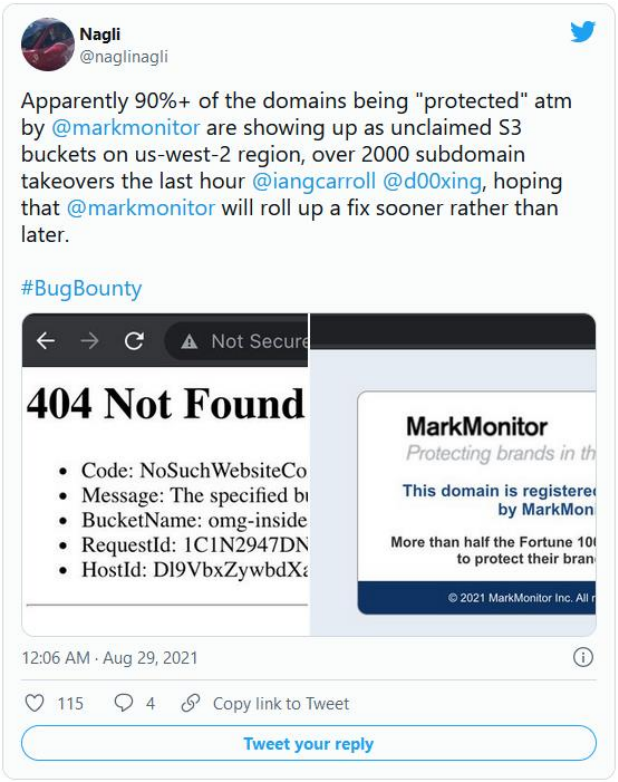
Domains previously showed 404 "NoSuchBucket" found errors from Amazon S3 servers
Source: BleepingComputer

An attacker can then take over the vulnerable domain in the sense that they can begin serving their own content at the location where the domain's dangling DNS entry is pointing to.

"If *testing.example.com* is pointed towards Amazon S3, what will S3 do if that bucket hasn't been created yet? It will just throw a 404 error—and wait for someone to claim it," explains Carroll.

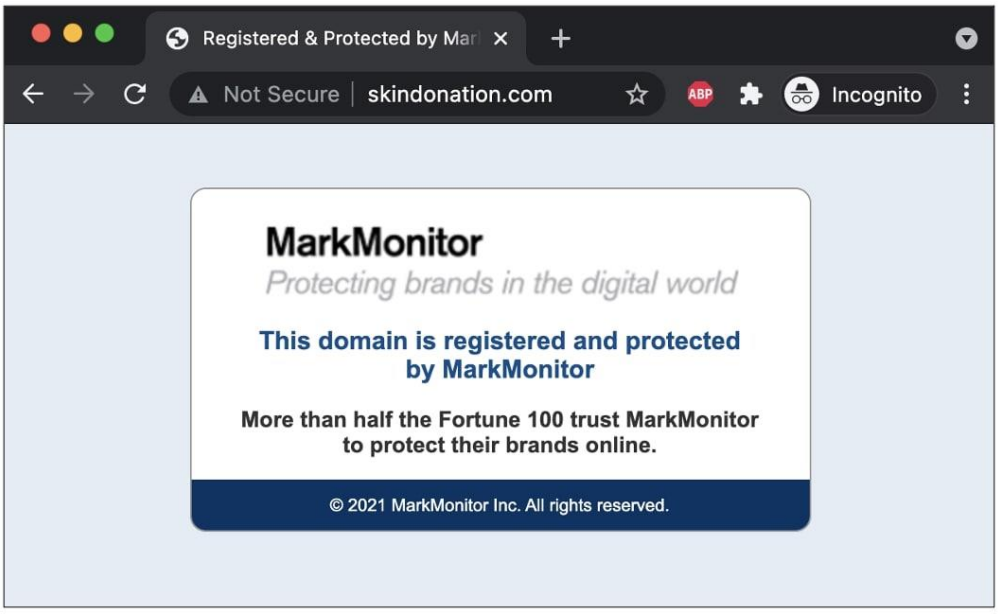
"If we claim this domain inside S3 before *example.com's* owners do, then we can claim the right to use it with S3 and upload anything we want," continues the engineer in his writeup.

That is exactly what happened when Carroll, along with other researchers, was able to take over more than 800 root domains, as a part of the research:



Issue impacted over 60,000 domains, lasted under an hour

After Carroll emailed MarkMonitor's security contact, the researcher did not hear back. But, he noticed that the domains previously throwing S3 "bucket not found" errors gradually started showing the proper MarkMonitor landing page:



MarkMonitor default parking page now visible for previously vulnerable domains
Source: BleepingComputer

"After I sent an email to security@markmonitor.com that went unacknowledged, domains stopped pointing to S3 over an hour after it began," says Carroll.

"I claimed over 800 root domains in this timeframe, and other researchers had similar amounts of claimed domains," continued the engineer.

Carroll's main concern was, as many as 62,000 domains parked over at MarkMonitor could potentially be hijacked, and abused for phishing.

For example, using intel-gathering service SecurityTrails, the engineer identified highly valuable domains representing known brand names, including google.ar and coinbase.ca that would make great phishing candidates, should these be taken over:

1 - 100 of 62,647 results « ‹ 1 2 3 4 5 › »

Add to downloads View downloads

domain.apex	rank.alexa
kindleer.com	18091
myfiosgateway.com	72866
paysafecorp.com	99304
waptw.com	127058
google.ar	152243
heetsguy.com	162852
summify.com	232086
hubspothero.com	295908
unblockyoutube.net	322036
wayfair.co	323889
google.co.om	424565
oneplatform.io	434710
alibaba.co	467277
coinbase.ca	468605
dropbox.com.my	484327

Highly ranked domains that could be potentially taken over for phishing
Source: Ian Carroll, via SecurityTrails

BleepingComputer reached out to both Amazon and MarkMonitor for learning more, and heard back from MarkMonitor's parent company, Clarivate:

"During a planned move of our parking page to the cloud, our DDoS protection vendor temporarily routed traffic in an unexpected manner for some domains using MarkMonitor's parking page service," a Clarivate spokesperson told BleepingComputer.

"Neither live domains nor DNS were impacted. We take the protection of the domains entrusted to us – including parked domains – extremely seriously, and we work every day to make sure we are following the best security practices and guidelines."

"This includes having active and static scanning, ongoing DNS monitoring, annual 3rd party penetration testing, and other security audits," continued Clarivate spokesperson.

Clarivate is also in the process of finalizing a bug bounty program.

MarkMonitor states, as soon as the unexpected behavior was identified, the company immediately reverted their DDoS vendor settings to point traffic to an internally-hosted web server's parked page.

Full detection, investigation, and remediation were completed in under an hour, says MarkMonitor.

Following their investigation, the registrar is not aware of any instances of malicious content being hosted for any parked page.

When asked what could companies do to better protect themselves against domain takeover weaknesses like these, Carroll said:

"Until cloud providers like Amazon move to prevent domain takeovers like this, companies need to be careful when pointing traffic to them, either via DNS records or otherwise," Carroll told BleepingComputer.

"This issue is not entirely the fault of MarkMonitor. While they need to be careful with handling parked domains, AWS is at fault for not being more stringent with claiming S3 buckets. Google Cloud, for example, has required domain verification for years, rendering this [attack] useless," says the engineer in his blog post.

Amazon did not respond to our request for comment.

MarkMonitor stated to BleepingComputer that they continuously review their test cases and policies to identify and be alerted of such issues.

"We are also evaluating mechanisms to be alerted more quickly of any HTTP error responses from domains that are parked with our parking service, which may allow us to identify and react to unexpected behavior even more quickly in the future," concluded MarkMonitor spokesperson in their statement to BleepingComputer.

Source: https://www.bleepingcomputer.com/news/security/over-60-000-parked-domains-were-vulnerable-to-aws-hijacking/

2. Hackers leak passwords for 500,000 Fortinet VPN accounts

A threat actor has leaked a list of almost 500,000 Fortinet VPN login names and passwords that were allegedly scraped from exploitable devices last summer.

While the threat actor states that the exploited Fortinet vulnerability has since been patched, they claim that many VPN credentials are still valid.

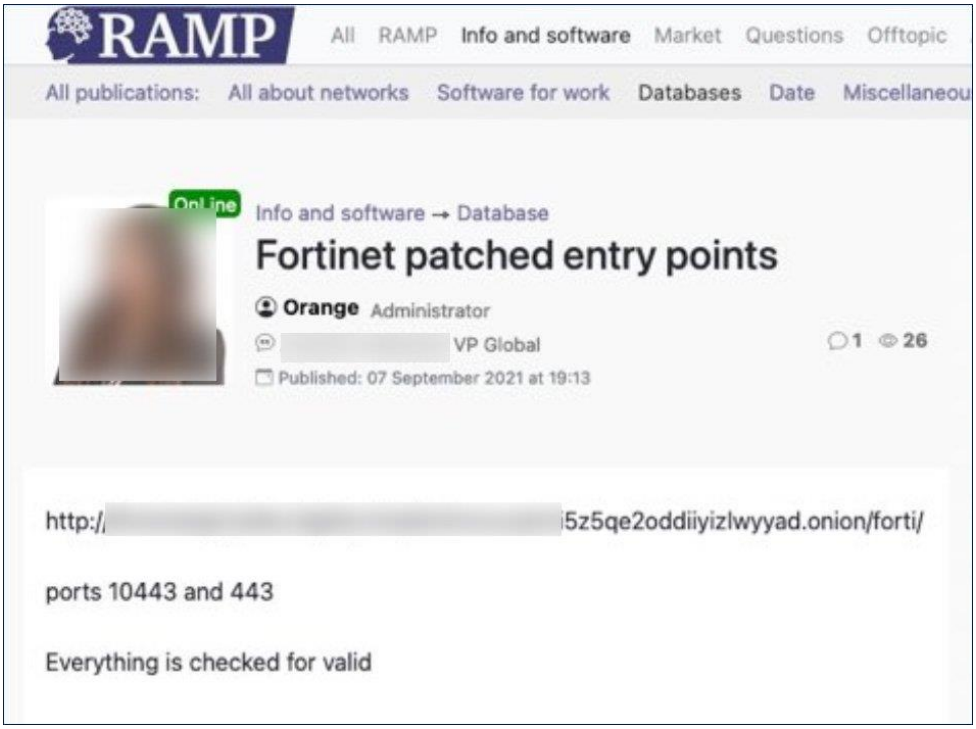
This leak is a serious incident as the VPN credentials could allow threat actors to access a network to perform data exfiltration, install malware, and perform ransomware attacks.

Fortinet credentials leaked on a hacking forum

The list of Fortinet credentials was leaked for free by a threat actor known as 'Orange,' who is the administrator of the newly launched RAMP hacking forum and a previous operator of the Babuk Ransomware operation.

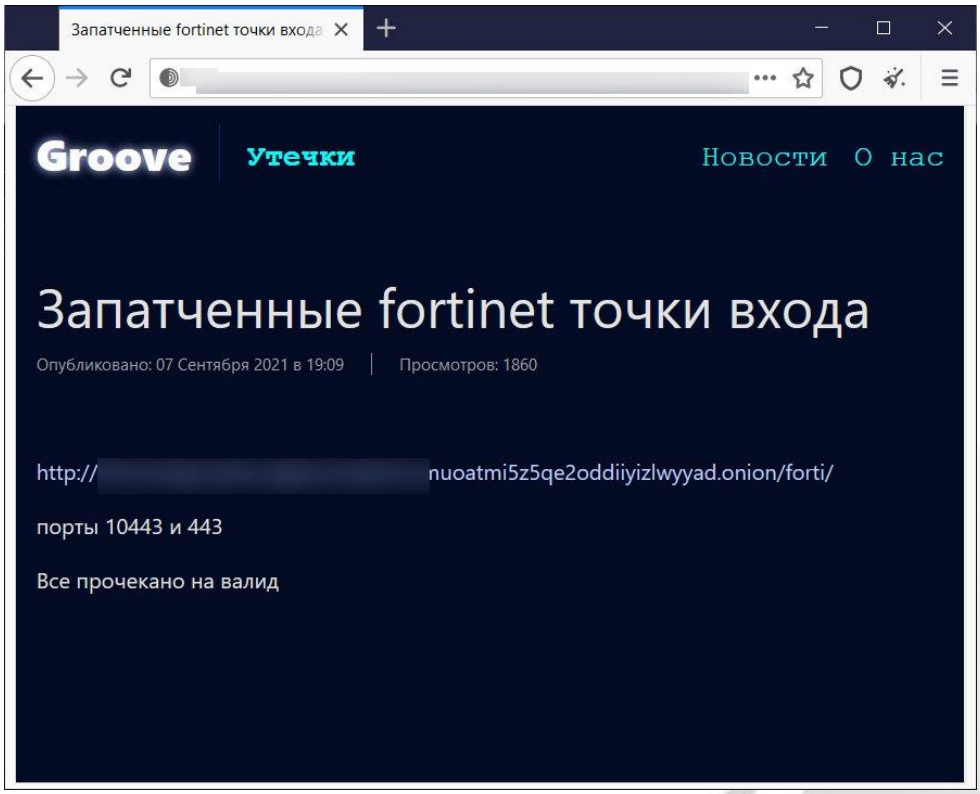
After disputes occurred between members of the Babuk gang, Orange split off to start RAMP and is now believed to be a representative of the new Groove ransomware operation.

Yesterday, the threat actor created a post on the RAMP forum with a link to a file that allegedly contains thousands of Fortinet VPN accounts.



Post on the RAMP hacking forum

At the same time, a post appeared on Groove ransomware's data leak site also promoting the Fortinet VPN leak.



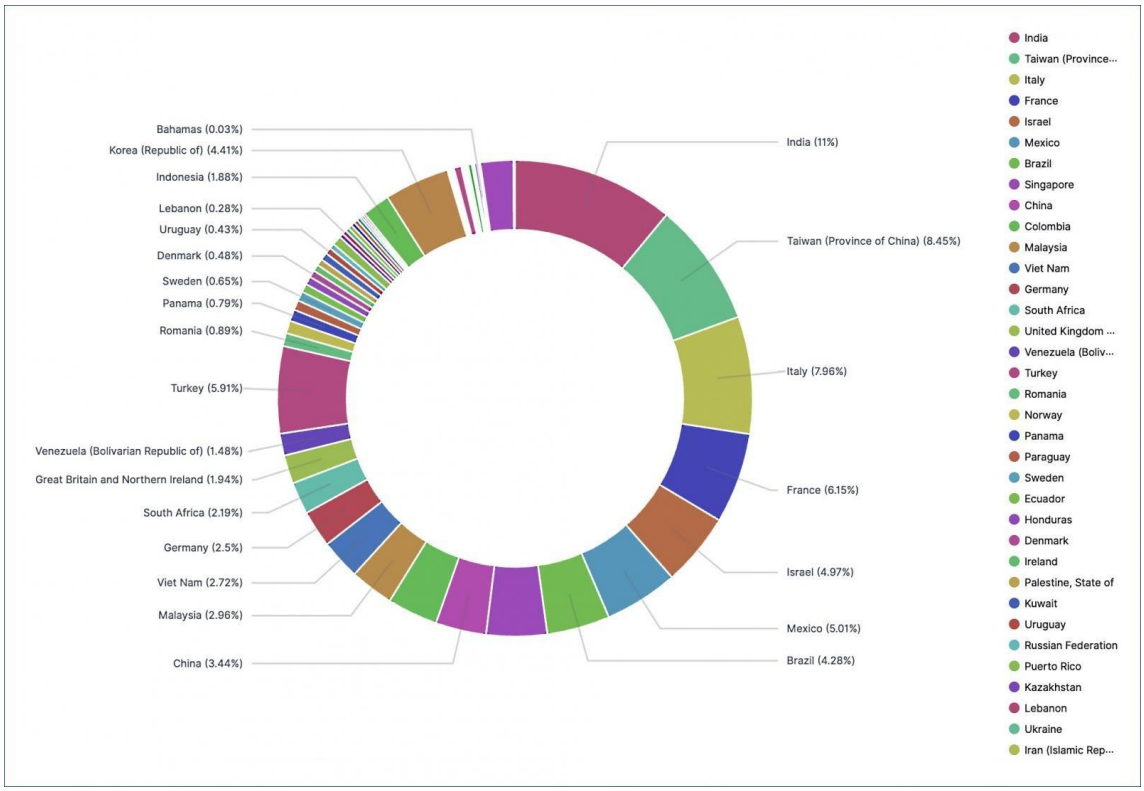
Post about the Fortinet leak on the Groove data leak site

Both posts lead to a file hosted on a Tor storage server used by the Groove gang to host stolen files leaked to pressure ransomware victims to pay.

BleepingComputer's analysis of this file shows that it contains VPN credentials for 498,908 users over 12,856 devices.

While we did not test if any of the leaked credentials were valid, BleepingComputer can confirm that all of the IP address we checked are Fortinet VPN servers.

Further analysis conducted by Advanced Intel shows that the IP addresses are for devices worldwide, with 2,959 devices located in the USA.



Geographic distribution of leaked Fortinet servers

Kremez told BleepingComputer that the now-patched Fortinet CVE-2018-13379 vulnerability was exploited to gather these credentials.

A source in the cybersecurity industry told BleepingComputer that they were able to legally verify that at least some of the leaked credentials were valid.

However some sources are giving mixed answers, with some saying many credentials work, while others state that most do not.

It is unclear why the threat actor released the credentials rather than using them for themselves, but it is believed to have been done to promote the RAMP hacking forum and the Groove ransomware-as-a-service operation.

"We believe with high confidence the VPN SSL leak was likely accomplished to promote the new RAMP ransomware forum offering a "freebie" for wannabe ransomware operators." Advanced Intel CTO Vitali Kremez told BleepingComputer.

Groove is a relatively new ransomware operation that only has one victim currently listed on their data leak site. However, by offering freebies to the cybercriminal community, they may be hoping to recruit other threat actors to their affiliate system.

What should Fortinet VPN server admins do?

While BleepingComputer cannot legally verify the list of credentials, if you are an administrator of Fortinet VPN servers, you should assume that many of the listed credentials are valid and take precautions.

These precautions include performing a forced reset of all user passwords to be safe and to check your logs for possible intrusions.

If anything looks suspicious, you should immediately make sure that you have the latest patches installed, perform a more thorough investigation, and make sure that your user's passwords are reset.

To check if a device is part of the leak, security researcher Cypher has created a list of the leaked device's IP addressees.

While Fortinet never responded to our emails about the leak, after we emailed them about the incident they published an advisory confirming our reporting that the leak was related to the CVE-2018-13379 vulnerability.

> *"This incident is related to an old vulnerability resolved in May 2019. At that time, Fortinet issued a PSIRT advisory and communicated directly with customers.*
>
> *And because customer security is our top priority, Fortinet subsequently issued multiple corporate blog posts detailing this issue, strongly encouraging customers to upgrade affected devices. In addition to advisories, bulletins, and direct communications, these blogs were published in August 2019, July 2020, April 2021, and again in June 2021." - Fortinet.*

Update 9/9/21: Added Fortinet's statement, mixed information about the validity of the credentials, and link to list of leaked device IP addresses.

Source: https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/

3. Microsoft rolls out passwordless login for all Microsoft accounts

Microsoft is rolling out passwordless login support over the coming weeks, allowing customers to sign in to Microsoft accounts without using a password.

The company first allowed commercial customers to rollout passwordless authentication in their environments in March after a breakthrough year in 2020 when Microsoft reported that over 150 million users were logging into their Azure Active Directory and Microsoft accounts without using a password.

Rolling out to all Microsoft accounts

Starting today, Redmond announced that users are no longer required to have a password on their accounts.

Instead, they can choose between the Microsoft Authenticator app, Windows Hello, a security key, or phone/email verification codes to log into Microsoft Edge or Microsoft 365 apps and services.

"Now you can remove the password from your Microsoft account and sign in using passwordless methods like Windows Hello, the Microsoft Authenticator mobile app or a verification code sent to your phone or email," said Liat Ben-Zur, Microsoft Corporate Vice President.

"This feature will help to protect your Microsoft account from identity attacks like phishing while providing even easier access to the best apps and services like Microsoft 365, Microsoft Teams, Outlook, OneDrive, Family Safety, Microsoft Edge and more."

As Microsoft Corporate Vice President for Security, Compliance, and Identity Vasu Jakkal added, threat actors use weak passwords as the initial attack vector in most attacks across enterprise and consumer accounts. Microsoft detects 579 password attacks every second, with a total of 18 billion incidents each year.

"One of our recent surveys found that 15 percent of people use their pets' names for password inspiration. Other common answers included family names and important dates like birthdays," Jakkal said.

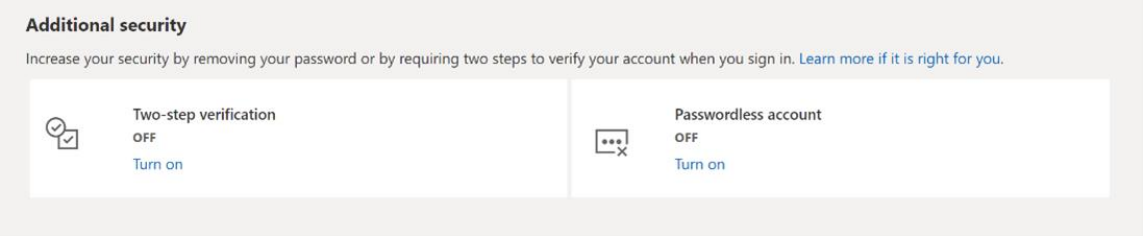
"We also found 1 in 10 people admitted reusing passwords across sites, and 40 percent say they've used a formula for their passwords, like Fall2021, which eventually becomes Winter2021 or Spring2022."

How to go passwordless right now

To start logging in to your Microsoft account without a password, you first need to install the Microsoft Authenticator app and link it to your personal Microsoft account.

Next, you have to go to your Microsoft account page, sign in, and turn on the 'Passwordless Account" under Advanced Security Options > Additional Security Options.

The last steps require you to follow the on-screen prompts and approve the notification displayed by the Authenticator app.



Passwordless account toggle (Microsoft)

More info on using a passwordless method to sign in to your account is available on Microsoft's support website.

"Passwordless solutions such as Windows Hello, the Microsoft Authenticator app, SMS or Email codes, and physical security keys provide a more secure and convenient sign-in method," Microsoft explains.

"While passwords can be guessed, stolen, or phished, only you can provide fingerprint authentication, or provide the right response on your mobile at the right time."

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-rolls-out-passwordless-login-for-all-microsoft-accounts/

4. No Patch for High-Severity Bug in Legacy IBM System X Servers

Two of IBM's aging flagship server models, retired in 2020, won't be patched for a command-injection flaw.

Two legacy IBM System x server models, retired in 2019, are open to attack and will not receive security patches, according to hardware maker Lenovo. However, the company is offering workaround mitigation.

The two models, IBM System x 3550 M3 and IBM System x 3650 M3, are both vulnerable to command injection attacks. The bug allows an adversary to execute arbitrary commands on either server model's operating system via a vulnerable application called Integrated Management Module (IMM).

IMM is used for systems-management functions. On the back panel of System x models, serial and Ethernet connectors use the IMM for device management. The flaw, according to a Lenovo advisory posted Tuesday, is in the IMM firmware code and "could allow the execution of operating system commands over an authenticated SSH or Telnet session."

SSH or Secure Shell is a cryptographic network communication protocol allowing two computers to communicate or share data. Telnet is another network protocol that allows remote users to log into another computer on the same network. Telnet, by default, does not encrypt data sent over its connection.

The bug, tracked as CVE-2021-3723, was disclosed on Wednesday and bug hunter Denver Abrey is credited for finding it.

Eight vulnerabilities in a later version of IMM – called IMM2 – were identified in June 2020, three high-severity. These bugs were tied to flaws in client-side code responsible for implementing the SSH2 protocol, called libssh2.

Both the System x 3550 M3 and System x 3650 M3 were introduced April 5, 2011 (PDF) as midsized businesses solutions. On June 30, 2015, Lenovo announced systems were both discontinued, but would receive security updates for five additional years.

According to the Lenovo security bulletin, software and security support for System x 3550 and 3650 ended December 31, 2019.

"Lenovo has historically provided service and support for at least five years following a product's withdrawal from marketing. This is subject to change at Lenovo's sole discretion without notice. Lenovo will announce a product's EOS date at least 90 days before the actual EOS date and in most cases longer," wrote Lenovo.

On Wednesday Lenovo said it "recommends discontinuation of use" of both servers, but offered a "mitigation strategy". [...]

Lenovo did not indicate if it was aware of any active campaigns targeting the vulnerability.

Source: https://threatpost.com/no-patch-for-ibm-system-x-servers/169491/

5. Billions more Android devices will reset risky app permissions

Google announced today that support for a recently released Android privacy protection feature would be backported to billions of devices running older Android versions later this year.

The permission auto-reset feature, first introduced with Android 11, is designed to protect users' privacy by automatically removing runtime permissions for apps that haven't been used for months.

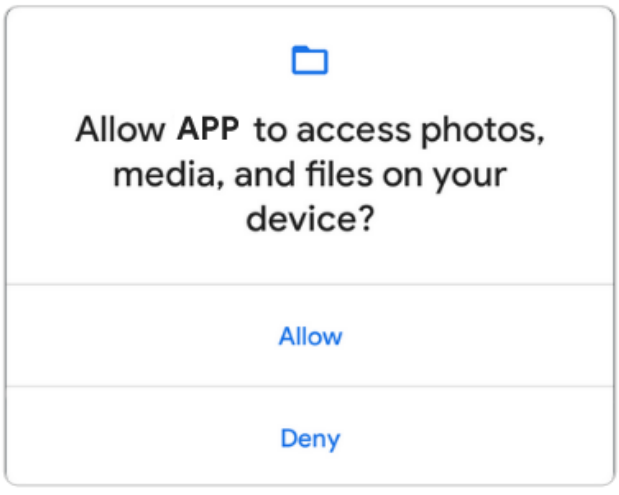
Runtime permissions (aka dangerous permissions), as Google explains, display prompts to request access to sensitive or private user data.

When this feature starts rolling out to older Android devices, it will be made available on all devices with Google Play services and running Android 6.0 (API level 23) up to and including Android 10 (API level 29).

"Starting in December 2021, we are expanding this to billions more devices. This feature will automatically be enabled on devices with Google Play services that are running Android 6.0 (API level 23) or higher," Google explained.

"On these devices, users can now go to the auto-reset settings page and enable/disable auto-reset for specific apps.

"The system will start to automatically reset the permissions of unused apps a few weeks after the feature launches on a device."



Runtime permissions prompt (Google)

Rolled out to all compatible devices until Q2 2022

While permission auto-reset will be enabled by default on Android 11 devices, users will be able to toggle it on manually on Android 6.0 or later.

The launch timeline starts with the auto-reset APIs (who were made available to developers in beta on September 15) being released as stable in October.

Gradual rollout across all devices powered by Google Play Services and running Android 6.0 or later will start in December 2021.

The rollout process will end in Q1 2022 when the feature is expected to reach all compatible Android devices.

In July, Google also started emailing Android users that they will no longer be able to log in to their Google accounts on devices running Android 2.3.7 (Gingerbread) and lower.

The Android OS now powers over 3 billion devices around the world as Google's VP of product management Sameer Samat revealed at this year's Google I/O annual developer conference.

Android 11, the current stable Android version was released last year, on September 8, 2020.

Source: https://www.bleepingcomputer.com/news/security/billions-more-android-devices-will-reset-risky-app-permissions/

6. TangleBot Malware Reaches Deep into Android Device Functions

The mobile baddie grants itself access to almost everything, enabling spying, data-harvesting, stalking and fraud attacks, among others.

An Android malware called TangleBot has weaved its way onto the cyber-scene: One that researchers said can perform a bouquet of malicious actions, including stealing personal info and controlling apps and device functions.

According to Cloudmark researchers, the newly discovered mobile malware is spreading via SMS messaging in the U.S. and Canada, using lures about COVID-19 boosters and regulations. The goal is to social-engineer targets into clicking on an embedded link, which takes them to a website. The site tells users they need an "Adobe Flash update." If they click on the subsequent dialog boxes, TangleBot malware installs.

In propagation and theme, TangleBot resembles other mobile malware, such as the FluBot SMS malware that targets the U.K. and Europe or the CovidLock Android ransomware, which is an Android app that pretends to give users a way to find nearby COVID-19 patients. But its wide-ranging access to mobile device functions is what sets it apart, Cloudmark researchers said.

"The malware has been given the moniker TangleBot because of its many levels of obfuscation and control over a myriad of entangled device functions, including contacts, SMS and phone capabilities, call logs, internet access, [GPS], and camera and microphone," they noted in a Thursday writeup.

To reach such a long arm into Android's internal business, TangleBot grants itself privileges to access and control all of the above, researchers said, meaning that the cyberattackers would now have carte blanche to mount attacks with a staggering array of goals.

For instance, attackers can manipulate the incoming voice call function to block calls and can also silently make calls in the background, with users none the wiser. That's a perfect setup for premium number fraud, where the user is charged a high rate for making a call to an attacker-controlled toll number.

TangleBot can also send, obtain and process text messages for SMS fraud, two-factor authentication interception, self-propagation to contacts and more.

It also has deep spyware capabilities, with the ability to record or directly stream camera, screen or microphone audio directly to the attacker, along with "other device observation capabilities," according to Cloudmark. Gaining access to the GPS functionality, for example, creates the potential for stalkery location-tracking.

And last but not least, the firm noted that the malware can take stock of installed applications and interact with them, as well as place overlay screens on top of these to, say, harvest credentials in the style of a banking trojan.

"The ability to detect installed apps, app interactions and inject overlay screens is extremely problematic," researchers noted. "As we have seen with FluBot, TangleBot can overlay banking or financial apps and directly steal the victim's account credentials….The capabilities also enable the theft of considerable personal information directly from the device."

That can be problematic for businesses, too, given that employees increasingly use personal devices for work.

To avoid threats like TangleBot, mobile users should practice safe messaging practices and avoid clicking on any links in texts, even if they appear to come from a legitimate contact, researchers noted. They should also be judicious when downloading apps and should read install prompts closely, looking out for information regarding rights and

privileges that the app may request. And finally, they should be wary of procuring any software from outside a certified app store.

"Harvesting of personal information and credentials in this manner is extremely troublesome for mobile users because there is a growing market on the Dark Web for detailed personal and account data," according to Cloudmark. "Even if the user discovers the TangleBot malware installed on their device and is able to remove it, the attacker may not use the stolen information for some period of time, rendering the victim oblivious of the theft."

Source: https://threatpost.com/tanglebot-malware-device-functions/174999/

7. Exchange/Outlook Autodiscover Bug Spills 100K+ Email Passwords

Hundreds of thousands of email credentials, many of which double as Active Directory domain credentials, came through to credential-trapping domains in clear text.

Guardicore security researcher Amit Serper has discovered a severe design bug in Microsoft Exchange's Autodiscover – a protocol that lets users easily configure applications such as Microsoft Outlook with just email addresses and passwords.

The flaw has caused the Autodiscover service to leak nearly 100,000 unique login names and passwords for Windows domains worldwide, Serper said in a technical report released this week.

"This is a severe security issue, since if an attacker can control such domains or has the ability to 'sniff' traffic in the same network, they can capture domain credentials in plain text (HTTP basic authentication) that are being transferred over the wire," he said.

"Moreover, if the attacker has DNS-poisoning capabilities on a large scale (such as a nation-state attacker), they could systematically syphon out leaky passwords through a large-scale DNS poisoning campaign based on these Autodiscover TLDs [top-level domains]," Serpa wrote.

The design flaw causes the protocol to leak web requests to Autodiscover domains outside of the user's own domain if they're in the same TLD – i.e., Autodiscover.com. Guardicore picked up a slew of those domains and found that researchers could set them up to intercept clear-text account credentials for hapless users experiencing network difficulties or whose admins goofed on configuring DNS.

Domain-buying Spree

Guardicore Labs picked up 11 Autodiscover domains with TLD suffixes that spanned the globe and which are listed below. Between April 16 and Aug. 25, 2021, researchers set up these domains to connect with a web server Guardicore controlled, thus configuring the domains to serve as proof-of-concept credential traps. [...]

Those credential traps opened the floodgate to "a massive" leak of valid Windows domain credentials, according to Serper's writeup. Over that four-month period, Guardicore captured 372,072 Windows domain credentials and 96,671 unique credentials leaked out of applications including Microsoft Outlook, mobile email clients and other apps that interface with Microsoft's Exchange server.

To top it all off, Guardicore developed an attack that downgrades a client's authentication scheme, elbowing it off of a secure one such as OAuth or HTLM and replacing it with HTTP Basic authentication, which sends credentials in clear text.

Thus, those hundreds of thousands of email credentials, many of which double as Active Directory domain credentials, came through to the credential-trapping domains in clear text.

The Problem: A POX Upon Your Protocol

The weakness Guardicore discovered has to do with a specific implementation of Autodiscover based on the POX (aka "plain old XML") XML protocol, through which applications exchange raw XML documents using standard transfer protocols such as HTTP, SMTP and FTP, or by using proprietary protocols, such as message-oriented middleware.

After adding a new Microsoft Exchange account to Outlook via its auto account setup, a prompt requests a user's username and password. After the user obliges, Outlook tries to use Autodiscover to configure the client.

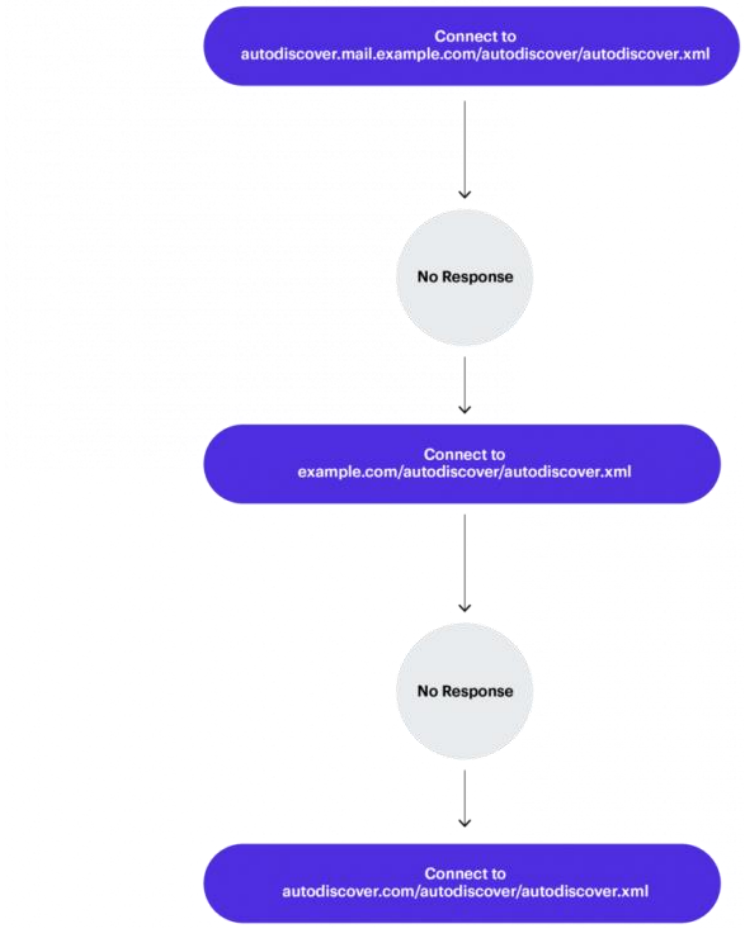
Autodiscover attempts to put together a URL to fetch configuration data based on the email domain in any of these formats that combine email domain, subdomain and a path string:

- https://Autodiscover.example.com/Autodiscover/Autodiscover.xml
- http://Autodiscover.example.com/Autodiscover/Autodiscover.xml
- https://example.com/Autodiscover/Autodiscover.xml
- http://example.com/Autodiscover/Autodiscover.xml

Failing that, it starts a "back-off" procedure, and therein lies the rub.

As Serper explained, this back-off mechanism "is the culprit of this leak because it is always trying to resolve the Autodiscover portion of the domain and it will always try to 'fail up,' so to speak."

On its next attempt to build an Autodiscover URL, the procedure would concoct "http://Autodiscover.com/Autodiscover/Autodiscover.xml," meaning that all of the requests that can't reach the original domain fall into the lap of whoever owns Autodiscover.com.



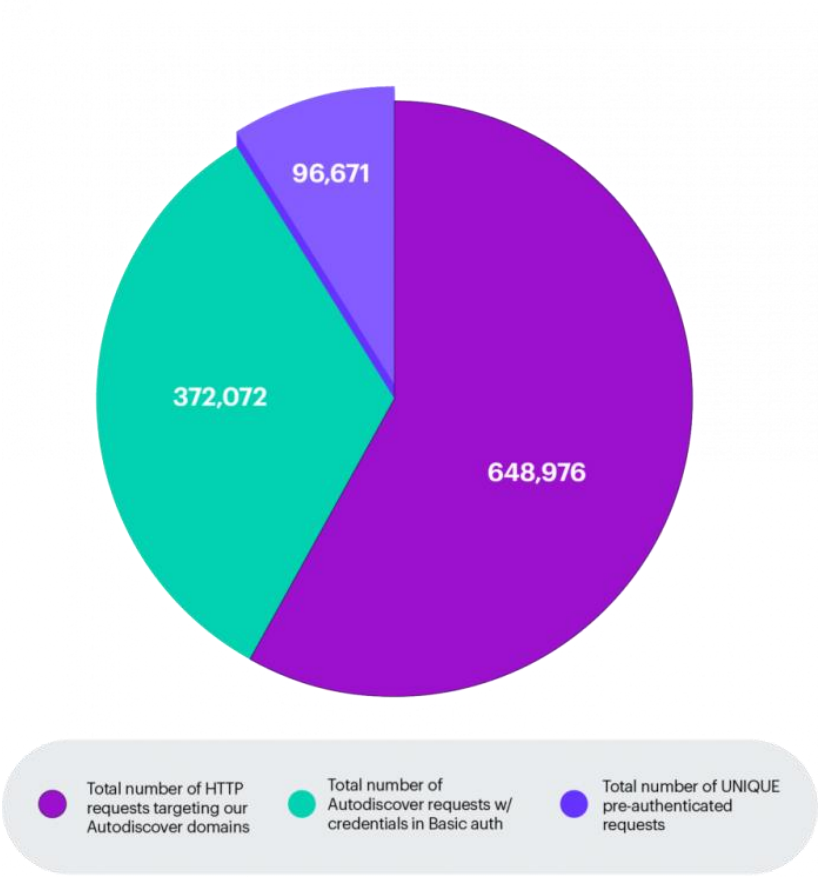
The Autodiscover back-off process. Source: Guardicore.

After the HTTP GET requests to its purchased domains started to arrive, Guardicore was surprised to discover that many requested the relative path of /Autodiscover/Autodiscover.xml with the Authorization header pre-populated with credentials.

"The interesting issue with a large amount of the requests that we received was that there was no attempt on the client's side to check if the resource is available, or even exists on the server, before sending an authenticated request," Serper commented. "Usually, the way to implement such a scenario would be to first check if the resource that the client is

requesting is valid, since it could be non existent (which will trigger an HTTP 404 error) or it may be password protected (which will trigger an HTTP 401 error code)."

He continued, "Between Apr 16, 2021 to Aug 25, 2021 we have captured a large number of credentials this way, needless to say, without sending a single packet other than what's required to establish an HTTP/HTTPS session between our server and the miscellaneous clients."



Requests breakdown. Source: Guardicore.

The requests – and their leaked credentials – came in from a wide range of sources: publicly traded Chinese companies, investment banks, food manufacturers, power plants, power delivery, real estate, shipping and logistics, and jewelry companies.

Given that Microsoft Exchange is part of Microsoft's "domain suite" of products, the fact that anybody who has credentials to log in to Exchange inboxes of such businesses – and, in most cases, also to their domain credentials – sets the stage for a world of cybersecurity hurt. "The implications of a domain credential leak in such scale are massive, and can put organizations in peril," Serber stressed. "Especially in today's ransomware-attacks ravaged-world – the easiest way for an attacker to gain entry into an organization is to use legitimate and valid credentials."

Guardicore sees a bit of irony in all this: Attackers try hard to weasel credentials out of users, be it through social engineering, phishing or what have you. This credentials leakage is like pennies from heaven for threat actors, though, coming as it does due to a design flaw in protocol meant to streamline IT operations when it comes to email client configuration. It "emphasises the importance of proper segmentation and Zero trust," Serper wrote.

A Design Flaw That's Been Known About for Years

As of Thursday, the flaw hadn't been patched, and Microsoft Senior Director Jeff Jones told Ars Technica that Guardicore disclosed the flaw publicly prior to reporting it to the company. But as a Guardicore spokesperson told Threatpost on Friday, it's not the first time that the flaw has been publicly reported.

"We did not notify Microsoft initially because the protocol flaw isn't new," the Guardicore representative said via email. "We were just able to exploit it at a massive scale."

In fact, as Guardicore's paper outlined, the flaw was discovered in 2017 by Shape Security and described in a paper that detailed how the leak can be caused by Autodiscover implementations on email clients on mobile phones, such as Samsung's email client on Android and Apple Mail on iOS (CVE-2016-9940, CVE-2017-2414).

Here we are, four years later, and the situation has just gotten worse, Guardicore said in the report:

> The vulnerabilities disclosed by Shape Security were patched, yet, here we are in 2021 with a significantly larger threat landscape, dealing with the exact same problem only with more third-party applications outside of email clients. These applications are exposing their users to the same risks. We have initiated responsible disclosure processes with some of the vendors affected. —Amit Serper, writing in Guardicore's report

In a Thursday Tweet stream, Serper called out Microsoft for lagging – for years – in its response to this known flaw. "Microsoft had plenty of time to fix or address this issue, either by patching products [or] just buying all of the autodiscover TLDs (which they are doing right now)," he wrote.

The researcher pointed to this flaw's history showing up in research papers (such as Shape Security's report), Black Hat conference talks (there was one such last month: It covered how Autodiscover formed a part of the ProxyShell vulnerabilities and attacks) and news articles ,"proving that these issues were known."

Microsoft hadn't responded to Threatpost's request for comment by the time this article was published. Guardicore is planning to release more details as a followup to the paper it released this week.

How to Plug the Leaks

Unfortunately, the news isn't great for the general public: After all, Autodiscover was designed to spare them from sinking up to their elbows in the guts of email client configuration, and mitigation requires rolling up shirtsleeves. [...]

The Buck Stops With Microsoft

Saryu Nayyar, CEO of risk-analytics provider Gurucul, told Threatpost that we can all thank our lucky stars that the credentials were grabbed by Guardicore – the "good guys," as she called them.

"That doesn't mean that we can rest easy, however," she cautioned. "If researchers understand the nature of the vulnerability and know how to exploit it, it's a short link to attackers exploiting it. Those organizations using detailed security analytics can easily determine if a login or access request is legitimate and investigate and remediate if necessary. This is a clear and severe weakness, but one that organizations can detect and respond to."

Alicia Townsend, technology evangelist at identity and access management firm OneLogin, told Threatpost that it seems "incredible" that a product would send a user's username and password to an untrusted endpoint.

"The fact that this is happening with an incredibly popular Microsoft product such as Exchange is even more disheartening," she noted. "But maybe the answer lies in the fact that it is happening in a product that has been around for so long."

Townsend pointed out that it's not clear how long this design flaw has been around, given that the Exchange Autodiscover feature was introduced in Exchange 2007. Regardless, it

doesn't shine a good light on Microsoft. "Whether the oversight was on the part of early developers or was introduced by more recent developers, it is clear that Security First was not their primary objective," she said.

The buck stops in Redmond, Townsend said. "It is the responsibility of all software manufacturers both on-prem and in the cloud to ensure that their developers are educated on how to create and test for secure code. We need to be continually evaluating our products for possible security risks. We need to evaluate not just new functionality but existing functionality, because as we can see with the Exchange Autodiscover feature, something could have been designed into the feature years ago and no one has been aware of it. Customers put their trust in us, and we need to be ever vigilant."

Source: https://threatpost.com/exchange-outlook-autodiscover-bug-spills-100k-email-passwords/175004/

8. Microsoft will disable Basic Auth in Exchange Online in October 2022

Microsoft announced that Basic Authentication will be turned off for all protocols in all tenants starting October 1st, 2022, to protect millions of Exchange Online users.

This announcement comes after the company postponed the removal of Basic Authentication from Exchange Online until the second half of 2021 because of the COVID-19 pandemic.

"Today, we are announcing that, effective October 1, 2022, we will begin to permanently disable Basic Auth in all tenants, regardless of usage (with the exception of SMTP Auth, which can still be re-enabled after that)," the Exchange Online Team said earlier this week.

Microsoft already began disabling basic auth in June for tenants who weren't using it and also explained how customers could re-enable protocols inadvertently affected.

To disable Basic Authentication in Exchange Online before Microsoft fully decommissions it, you need to create and assign auth policies to individual users using the steps detailed on the Exchange Online support website.

"Disabling Basic Authentication and requiring Modern Authentication with MFA is one of the best things you can do to improve the security of data in your tenant, and that has to be a good thing," Microsoft said two years ago when it revealed modern auth will be enforced across Exchange Online tenants.

"The last thing to make clear - this change only affects Exchange Online, we are not changing anything in the Exchange Server on-premises products."

Why is basic auth being disabled?

While Microsoft did not provide the exact reason why they decided to make this announcement this week, the cause is likely a Guardicore report that revealed how hundreds of thousands of Windows domain credentials were leaked in plain text by misconfigured email clients using basic auth.

Amit Serper, Guardicore's AVP of Security Research who authored the report, also disclosed an attack called the 'The ol' switcheroo' that forces an Exchange client to negotiate in basic authentication. [...]

Basic Authentication (also known as proxy authentication) is an HTTP-based authentication scheme through which apps send credentials with every connection request made to servers, endpoints, or online services, with the username/password pairs often stored locally on the device.

While it dramatically simplifies the authentication process, basic auth also makes it easier for attackers to steal the credentials when the connections are not secured using the Transport Layer Security (TLS) cryptographic protocol.

To make things even worse, enabling multi-factor authentication (MFA) is not easy when using basic auth; therefore, it often isn't used at all.

Modern Authentication (Active Directory Authentication Library (ADAL) and OAuth 2.0 token-based authentication) allows apps to use OAuth access tokens with a limited lifetime and can't be re-used to authenticate on other resources besides those that they were issued for.

After modern auth is toggled on, enabling and enforcing MFA will become more straightforward, with improved data security in Exchange Online as a direct and immediate result.

A demo video on adding MFA to Exchange Online/on-premises mailboxes is available on the Microsoft Ignite YouTube account.

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-will-disable-basic-auth-in-exchange-online-in-october-2022/

9. 5 Steps to Securing Your Network Perimeter

Ekaterina Kilyusheva, head of the Information Security Analytics Research Group at Positive Technologies, offers a blueprint for locking up the fortress.

When it comes to security, some of tomorrow's biggest threats will come from yesterday's vulnerabilities. In that regard, the network perimeter is a primary concern.

Network security has been discussed for years, and many best practices are well documented. And yet, according to Positive Technologies research, 84 percent of companies still have high-risk vulnerabilities on the perimeter, more than half (58 percent) have high-risk flaws with publicly available exploits, and – alarmingly — 26 percent are still vulnerable to WannaCry.

All of these factors, combined with the switch to remote work, have caused an increase in attacks exploiting vulnerabilities on the network perimeter, from five percent in Q1 2020 to 26 percent in the same quarter this year. One reason why companies can become targets is because low-skilled hackers often sell network access to more experienced criminal groups, such as ransomware operators. Exploits are now available for 10 percent of vulnerabilities detected on the perimeter, and that means even those without professional programming skills or experience in reverse engineering can exploit them.

So what measures should be taken to protect the network perimeter today, and which flaws are most commonly present in companies?

Step 1. Get Rid of the Deadwood

During a security assessment, even a cursory glance at any company's services available online can say a lot about its security level. If only a few services are available, they're usually protected by secure configuration and recent software updates that significantly facilitate eventual reconfiguration. Building a secure perimeter must start from resource inventory–in other words, from detecting and disabling active services that are not being used, as well as insecure protocols, and making sure that accessible interfaces truly need to be available online.

Which services are most frequently available to attackers? In Positive Technologies testing, we found every single company had TCP network ports 80 and 443 open on the perimeter. As a rule, these network ports have applications running on Apache HTTP Server, Apache Tomcat, Nginx and other web servers. By identifying a web server and its version, attackers can select relevant exploits.

Our research proved that 16 percent of web-server vulnerabilities have publicly available exploits. The availability of TCP network port 80 means that data can be exchanged via the HTTP protocol. And as we know, HTTP traffic is transmitted without encryption, meaning attackers can intercept it.

Analysis also revealed remote access and administration interfaces available on numerous resources, such as SSH, RDP or Telnet. Having these interfaces available to everyone on the internet is dangerous because they can allow any criminal to conduct brute-force attacks, so access to them should be limited.

Let's remember that attacks on remote-access services have been among the main cybercrime trends of 2020 and 2021. Organizations should also abandon the use of Telnet (which was found in 21 percent of companies), because it transmits credentials in cleartext,

and replace it with SSH. To make SSH connections more secure, use public key authentication, block SSH access for the root account, and use a non-standard port to guard against mass automated attacks.

At 84 percent of companies, TCP port 25 is open with the SMTP email service available on the perimeter. Data is transmitted in cleartext via SMTP, which means that just like with HTTP, attackers can intercept traffic and read corporate emails. In addition, insecure configuration of mail servers may leak corporate email addresses. The collected corporate email addresses can be used to brute-force credentials for network perimeter resources or remote access to the internal network, or to send phishing emails.

Step 2. Keep Software Up-to-Date

Positive Technologies research found that almost half of all detected vulnerabilities (47 percent) can be eliminated by simply installing the latest software updates. However, the same research also found that all companies had problems with keeping software up to date.

In fact, we found software that had reached its end of life at 42 percent of organizations, and we know at that point, developers stop releasing security updates. For example, 32 percent of companies still use PHP 5 applications, even though support for that language ended in January 2019.

As a result, 30 percent of vulnerabilities detected in outdated software versions and web-application code are among the most dangerous program code errors, according to MITRE. This MITRE ranking includes the most common critical errors that can be easily found and exploited by attackers in order to steal information, cause denial of service, or obtain full control over a vulnerable application.

Our research into network vulnerabilities also found that more than half of companies have vulnerabilities allowing execution of arbitrary code on the server, and 16 percent of these flaws have publicly available exploits, meaning the organizations had not patched for known vulnerabilities.

Almost two-thirds (64 percent) of these vulnerabilities are of high severity. The most common vulnerability was CVE-2017-12617 in Apache Tomcat, which is dangerous because attackers can exploit it to upload a JSP file to a vulnerable server and execute code contained in this file.

In the worst case, this could let attackers breach the network perimeter and access the local network, opening up the possibility for them to then steal confidential data, encrypt files with ransomware, gain access to critical business systems or obtain full control over the infrastructure.

Step 3. Make Sure Configurations Are Safe

Positive Technologies testing of network perimeters found that all companies had hosts that disclosed technical information: The contents of configuration files, routing to scanned hosts, OS versions and supported protocol versions.

The more information about the system attackers can collect, the higher the chance of a successful attack. Insecure configuration of services can also cause data leaks: For example, criminals can swipe detailed information about the system if the Community String value for the SNMP protocol — normally used to monitor various settings of network devices — is set as public or private. Ensure that all interfaces are configured securely.

Pay particular attention to the versions of supported protocols. For example, insecure versions of the SSL/TLS protocol can lead to disclosure of confidential information (see vulnerabilities CVE-2016-2183, CVE-2014-3566 and CVE-2013-2566).

Keep in mind that some vulnerabilities are related to the use of weak cryptographic mechanisms and keys. SSL certificates of 68 percent of companies use SHA-1 and MD5 hash functions. There are well-known attacks aimed at exploiting collisions in these algorithms, allowing attackers to compromise the certificate.

And, certificates at 53 percent of companies use RSA keys with a length of 1,024 bits or less. A weak secret RSA key in SSL/TLS allows an attacker to intercept a session by masquerading as a legitimate server. The recommended NIST length of an RSA key is at least 2,048 bits, so be sure to use strong cryptography.

Step 4. Use an Effective Vulnerability Management Process

International vulnerability databases annually publish information about thousands of new flaws. In addition, corporate IT infrastructures constantly go through changes, each of which potentially entails a security risk. All this makes vulnerability management a complex task.

Ensuring effective vulnerability management requires proper instrumental solutions, but with modern security assessment tools, companies can go beyond automating resource inventories and vulnerability searches to assess security policy compliance across the entire infrastructure.

Step 5. Test the Robustness of the Perimeter

Combine automated scanning with penetration testing. Automated scanning is only the first step toward achieving an acceptable level of security; subsequent steps should include verification, triage and remediation of risks and their causes.

Some of these steps represent common sense, while others require a concerted strategy matched with enforced policies. But they are all necessary. The network perimeter is a dynamic arena — if the situation isn't made better with effective security, it will surely get worse.

Source: https://threatpost.com/securing-network-perimeter/175043/

10. Working exploit released for VMware vCenter CVE-2021-22005 bug

A complete exploit for the remote code execution vulnerability in VMware vCenter tracked as CVE-2021-22005 is now widely available, and threat actors are taking advantage of it.

Unlike the version that started to circulate at the end of last week, this variant can be used to open a reverse shell on a vulnerable system, allowing remote attackers to execute code of their choice.

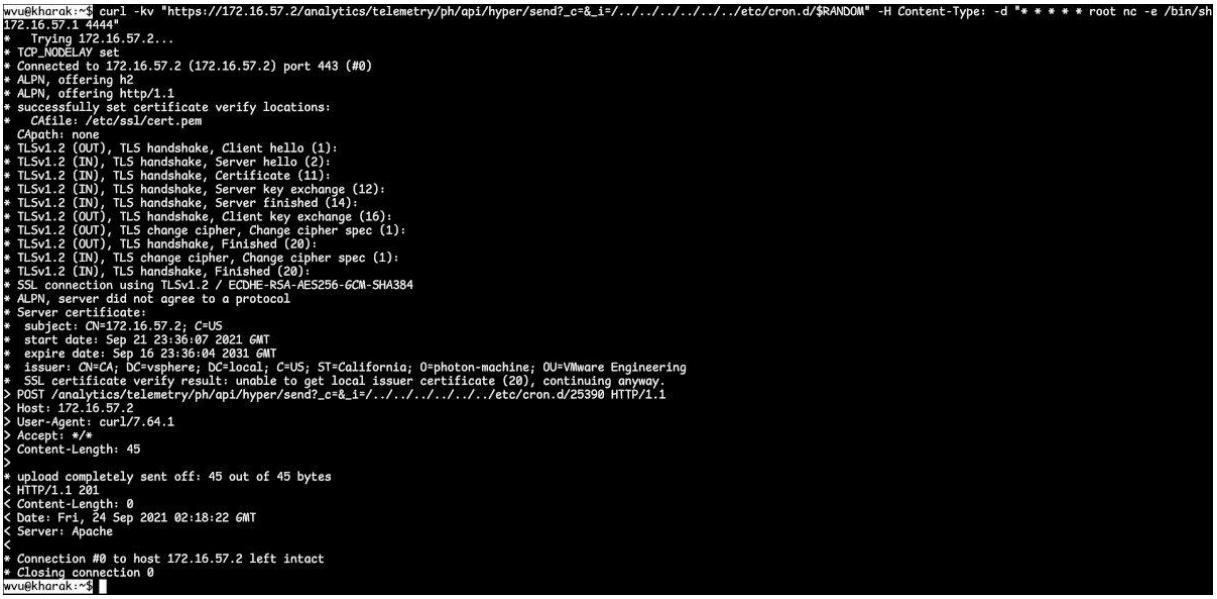
The vulnerability does not require authentication and allows attackers to upload a file to the vCenter Server analytics service.

Fully-working exploit at the ready

On Monday, exploit writer wvu released an unredacted exploit for CVE-2021-22005 that works against endpoints with the Customer Experience Improvement Program (CEIP) component enabled, which is the default state.

However, VMware describes the vulnerability as being exploitable "by anyone who can reach vCenter Server over the network to gain access, regardless of the configuration settings of vCenter Server."

In a technical analysis unlocked this week, wvu explains what their code does at each step, starting with a request that creates the directory needed for path traversal and scheduling the spawn of a reverse shell.



source: wvu

The researcher notes that although the exploit generates multiple files, the attack is not logged by typical solutions and recommends using the Audit framework, which collects data on both security and non-security relevant events.

VMware's advisory states that CVE-2021-22005 could be exploited "by anyone who can reach vCenter Server over the network," results from search engines indexing machines exposed on the public internet showed thousands of VMware vCenter hosts accessible over the web.

Prioritize installing the patch

VMware announced CVE-2021-22005 on September 21 with a critical severity rating of 9.8 out of 10 and a strong recommendation for organizations to consider "an emergency change" as per ITIL best practices of managing IT services, and patch "as soon as possible."

In an advisory on Friday, CISA also urged critical infrastructure organizations with vulnerable vCenter servers to prioritize updating the machines or to apply the temporary workaround from VMware.

Four days later, the first proof-of-concept exploit code became available. Although inert in its original state, the code could easily be weaponized to achieve remote code execution and attacks began shortly after its release.

After analyzing the incomplete code, CERT/CC vulnerability analyst Will Dormann noted that "the missing part from this PoC will indeed keep away script kiddies, but not any determined actor," adding that a complete exploit should emerge soon.

Threat actors have shown interest in this vulnerability early on, just hours after VMware disclosed it, and they quickly built a working exploit from the incomplete code that security researcher Jang released last week along with some technical notes.

With a fully-working exploit now available, the number of attacks are expected to increase as less-skilled actors can get involved. One of the highest risks for an organization is to become the victim of a ransomware attack, VMware warns.

Source: https://www.bleepingcomputer.com/news/security/working-exploit-released-for-vmware-vcenter-cve-2021-22005-bug/

11. Threat Actors Weaponize Telegram Bots to Compromise PayPal Accounts

A campaign is stealing one-time password tokens to gain access to PayPal, Apple Pay and Google Pay, among others.

Cybercriminals are using Telegram bots to steal one-time password tokens (OTPs) and defraud people through banks and online payment systems, including PayPal, Apple Pay and Google Pay, new research has found.

Researchers from Intel 471 discovered the campaign, which has been operational since June, they said in a report published Wednesday.

"Two-factor authentication is one of the easiest ways for people to protect any online account," researchers noted in the post. "So, of course criminals are trying to circumvent that protection."

Threat actors are using Telegram bots and channels and a range of tactics to gain account information, including calling victims, and impersonating banks and legitimate services, researchers said.

Through social engineering, threat actors also deceive people into giving them an OTP or other verification code via a mobile device, which the crooks then use to defraud accounts of money, they said.

"The ease by which attackers can use these bots can not be understated," they wrote in the report. "While there's some programming ability needed to create the bots, a bot user only needs to spend money to access the bot, obtain a phone number for a target, and then click a few buttons."

Indeed, Telegram bots have become a popular tool for cybercriminals, which have used them in various ways as part of user scams. A similar campaign discovered in January, dubbed Classiscam, where bots were sold as-a-service by Russian-speaking cybercriminals for the purpose of stealing money and payment data from European

victims. Other threat actors have been found using Telegram bots in a rather unique way as command-and-control for spyware.

In this case, Intel 471 researchers observed and analyzed the campaign's activity in regard to three bots—dubbed SMSRanger, BloodOTPbot and SMS Buster.

Easy-to-Use Bot as-a-Service

Researchers characterized SMSRanger as "easy to use," according to the post. Actors pay to access the bot and then can use it by entering commands, in a similar fashion to how bots are used on the widely used workforce collaboration platform Slack, they explained.

"A simple slash command allows a user to enable various 'modes' — scripts aimed as various services — that can target specific banks, as well as PayPal, Apple Pay, Google Pay or a wireless carrier," researchers wrote.

SMSRanger sends a potential victim a text message requesting his or her phone number, researchers said. Once a target's phone number has been entered in a chat message, the bot takes over from there, "ultimately granting [cybercriminals] access to whatever account has been targeted," they wrote.

About 80 percent of users who are targeted by SMSRanger will end up providing their full and accurate information to threat actors, allowing them to defraud these victims, researchers added.

Impersonating Trusted Companies

Meanwhile, BloodTPbot also uses the ability to send users a fraudulent OTP code via SMS, researchers noted. However, this bot requires an attacker to spoof the victim's phone number and impersonate a bank or company representative.

The bot attempts to call victims and uses social-engineering techniques to obtain a verification code from the person targeted. An attacker will receive a notification from the bot during the call specifying when to request the OTP during the authentication process, researchers explained. The bot then texts the code to the operator once the victim receives the OTP and enters it on the phone's keyboard.

BloodTPbot goes for a monthly fee of $300; users also can pay between $20 to $100 more to access live phishing panels that target accounts on social-media networks, including Facebook, Instagram and Snapchat; financial services like PayPal and Venmo; the investment app Robinhood; and cryptocurrency marketplace Coinbase, researchers said.

Masquerading as Banks

The third bot observed by researchers, SMS Buster, requires a bit more effort than the others for a threat actor to gain access to someone's account information, they said.

The bot provides options so an attacker can disguise a call made from any phone number to make it appear as a legitimate contact from a specific bank, researchers said. Upon calling a potential victim, an attackers follows a script to try to fool the target into providing info such as an ATM card PIN, credit card verification value (CVV) or OTP.

Researchers observed threat actors using SMS Buster against Canadian victims and their bank accounts, using both English and French to target people, they said. At the time the post was written, Intel 471 researchers had witnessed attackers illegally accessing accounts at eight different Canadian-based banks using SMS Buster.

"Overall, the bots show that some forms of two-factor authentication can have their own security risks," researchers concluded. "While SMS- and phone-call-based OTP services are better than nothing, criminals have found ways to socially engineer their way around the safeguards."

Source :https://threatpost.com/telegram-bots-compromise-paypal/175099/

12. GriftHorse Money-Stealing Trojan Takes 10M Android Users for a Ride

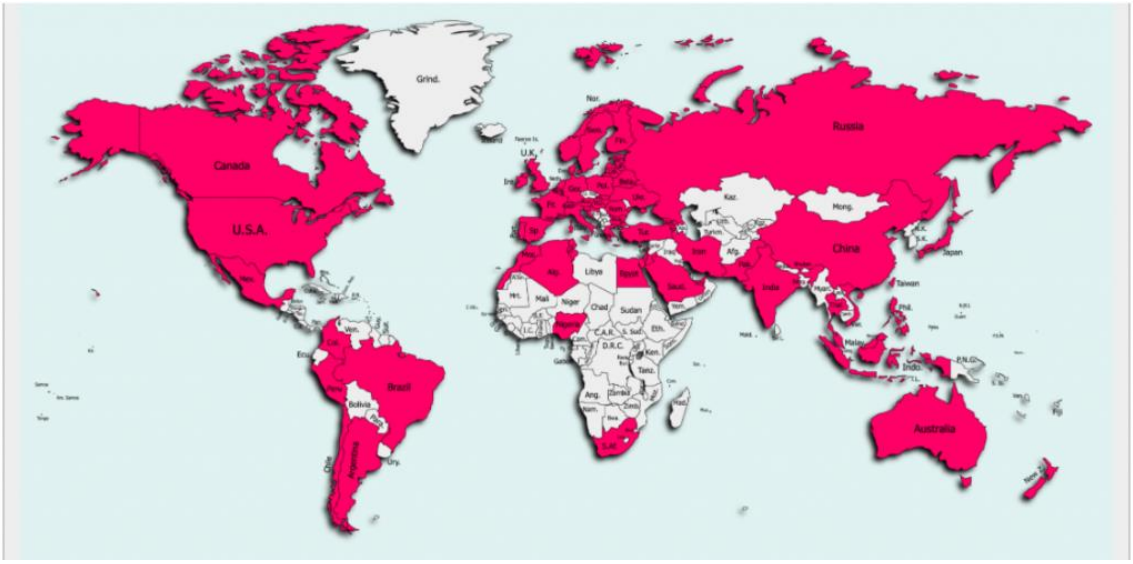
The mobile malware has fleeced hundreds of millions of dollars from victims globally, using sophisticated techniques.

More than 10 million Android users have been saddled with a malware called GriftHorse that's trojanizing various applications and secretly subscribing victims to premium mobile services – a type of billing fraud that researchers categorize as "fleeceware."

Zimperium uncovered more than 130 GriftHorse apps being distributed through both Google Play and third-party application stores, across all categories. Some of them have basic functionality, and some of them do nothing, researchers said. In either case, once installed, they lead to victims being billed for premium services – but phone-owners are usually none the wiser until they take a look at their mobile bills.

GriftHorse rode onto the scene in November of last year, and by now, "the total amount stolen could be well into the hundreds of millions of Euros," according to Zimperium researchers, with each victim paying upwards of $40 per month.

Victims sprawl across 70 different countries, all packing sneaky extra charges that they may not be aware of. Google removed the flagged apps, but GriftHorse is far from corralled: There could be additional Play apps, installs could still be active on peoples' phones, and the apps remain in many unofficial stores.



Distribution of GriftHorse Android malware victims. Source: Zimperium.

If users are unlucky enough to download one of the apps, they'll find themselves "bombarded with alerts on the screen letting them know they had won a prize and need to claim it immediately," according to Zimperium's Wednesday analysis. "These pop ups reappear no less than five times per hour until the application user successfully accepts the offer."

This is where it gets sneaky: Upon accepting the invitation for the prize, the malware serves victims selective pages, based on the geolocation of their IP addresses, using the local language and targeted verbiage. Those pages are also dynamically generated to avoid the blacklisting of strings by security solutions.

"These cybercriminals took great care not to get caught by malware researchers by avoiding hardcoding URLs or reusing the same domains, and filtering/serving the malicious payload based on the originating IP address's geolocation," according to the researchers. "This method allowed the attackers to target different countries in different ways. This check on the server-side evades dynamic analysis checking for network communication and behaviors."

The redirect page asks targets to submit their phone numbers for "verification." In reality, typing in the numbers merely subscribes them to a premium SMS service that charges $42 on average per month (€36), which will show up on their phone bills.

Looking GriftHorse in the Mouth

The creators of the apps have employed several novel techniques to help the apps stay off the radar of security vendors, the analysis found. In addition to the no-reuse policy for URLs mentioned above, the cybercriminals are also developing the apps using Apache Cordova.

Cordova allows developers to use standard web technologies – HTML5, CSS3 and JavaScript – for cross-platform mobile development – which in turn allows them to push out updates to apps without requiring user interaction.

"[This] technology can be abused to host the malicious code on the server and develop an application that executes this code in real-time," according to Zimperium. "The application displays as a web page that references HTML, CSS, JavaScript and images."

The campaign is also supported with a sophisticated architecture and plenty of encryption, which makes detection more difficult, according to the researchers.

For instance, when an app is launched, the encrypted files stored in the "assets/www" folder are decrypted using AES. After a bit more unpacking, the core functionality source code uses the GetData() function to establish communication between the application and a first-stage command-and-control (C2) server by encrypting an HTTP POST request.

The app then receives an encrypted response, which is decrypted using AES to collect a second-stage C2 URL. It also executes a GET request using Cordova's "InAppBrowser" function to uncover a third-stage URL, and it starts pushing user notifications about the supposed "prize" once an hour, five times in a row, according to the analysis.

"The second-stage C2 domain is always the same irrespective of the application or the geolocation of the victim," researchers explained. "The third-stage URL displays the final page asking for the victim's phone number and subscribes to several paid services and premium subscriptions."

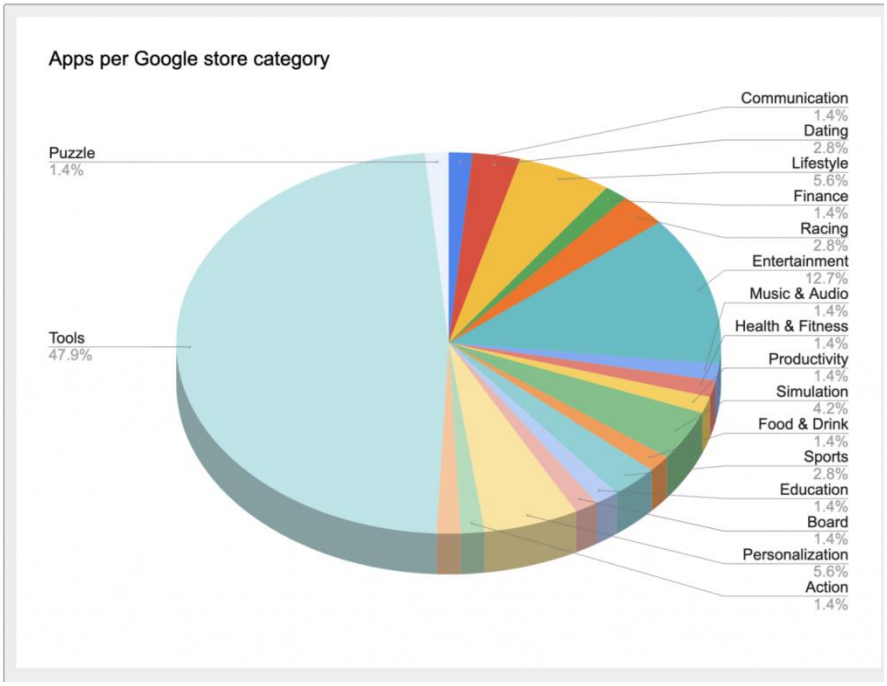
JavaScript code embedded in the page is responsible for the malicious behavior of the application, researchers added: "The interaction between the WebPage and the in-app functions is facilitated by the JavaScript Interface, which allows JavaScript code inside a WebView to trigger actions in the native (application-level) code. This can include the collection of data about the device, including IMEI and IMSI among others."

Android Fleeceware Continues to Plague Users

GriftHorse is not the only malware that looks to defraud victims via trojanized apps. The well-documented Joker malware, for example, has been circulating since 2017, disguising itself within hundreds of common, legitimate apps like camera apps, games, messengers, photo editors, translators and wallpapers.

Once installed, Joker silently simulates clicks and intercepts SMS messages to – you guessed it – subscribe victims to unwanted, paid premium services controlled by the attackers. The apps also steal SMS messages, contact lists and device information.

GriftHorse takes a slightly different approach than Joker, but Zimperium warned that it's just as virulent.



Source: Zimperium.

"The threat actors have exerted substantial effort to maximize their presence in the Android ecosystem through a large number of applications, developer accounts and domains," they said. "The GriftHorse campaign is one of the most widespread campaigns the zLabs threat research team has witnessed in 2021. The cybercriminal group behind the GriftHorse campaign has built a stable cash flow of illicit funds from these victims, generating millions in recurring revenue each month with the total amount stolen potentially well into the hundreds of millions."

Source: https://threatpost.com/grifthorse-money-stealing-trojan-android/175130/

13. Facebook open-sources tool to find Android app security flaws

Facebook today open-sourced a static analysis tool its software and security engineers use internally to find potentially dangerous security and privacy flaws in the company's Android and Java applications.

This security-focused tool, dubbed Mariana Trench (MT), can analyze large codebases of tens of millions of lines of code to spot vulnerabilities before they're introduced in the codebase.

Facebook revealed that its engineers found more than 50% of all security bugs across the company's apps using automated tools similar to Mariana Trench.

How it works

Mariana Trench works by analyzing the information flow from "sources" (user sensitive data such as passwords or locations) to "sinks" (functions or methods using data originating from sources).

Mariana Trench is specifically designed to automatically discover such issues, which, in most cases, could lead to severe privacy and security bugs.

"By default Mariana Trench analyzes dalvik bytecode and can work with or without access to the source code," Facebook explains on the tool's documentation website.

"A flow from sources to sinks indicate that for example user passwords may get logged into a file, which is not desirable and is called as an 'issue' under the context of Mariana Trench," Facebook Software Engineer Dominik Gabi said.

Developers and engineers can use the tool to focus on specific security and privacy issues by adjusting and training it by adding new rules and model generators so that it homes in on the areas sensitive data shouldn't end up.

Third code analysis tool open-sourced since 2019

The company previously released two other static code analysis tools designed to detect and prevent security issues for Python code (Pysa) and Hack code (Zoncolan).

You can find the Mariana Trench code analysis tool on GitHub and its own dedicated website, a binary distribution on PyPI, and a short tutorial to help get started.

'We built MT to focus particularly on Android applications. There are differences in patching and ensuring the adoption of code updates between mobile and web applications, so they require different approaches," Gabi added.

"While server-side code can be updated almost instantaneously for web apps, mitigating a security bug in an Android application relies on each user updating the application on the device they own in a timely way.

"This makes it that much more important for any app developer to put systems in place to help prevent vulnerabilities from making it into mobile releases, whenever possible."

Source: https://www.bleepingcomputer.com/news/security/facebook-open-sources-tool-to-find-android-app-security-flaws/

14. Google pushes emergency Chrome update to fix two zero-days

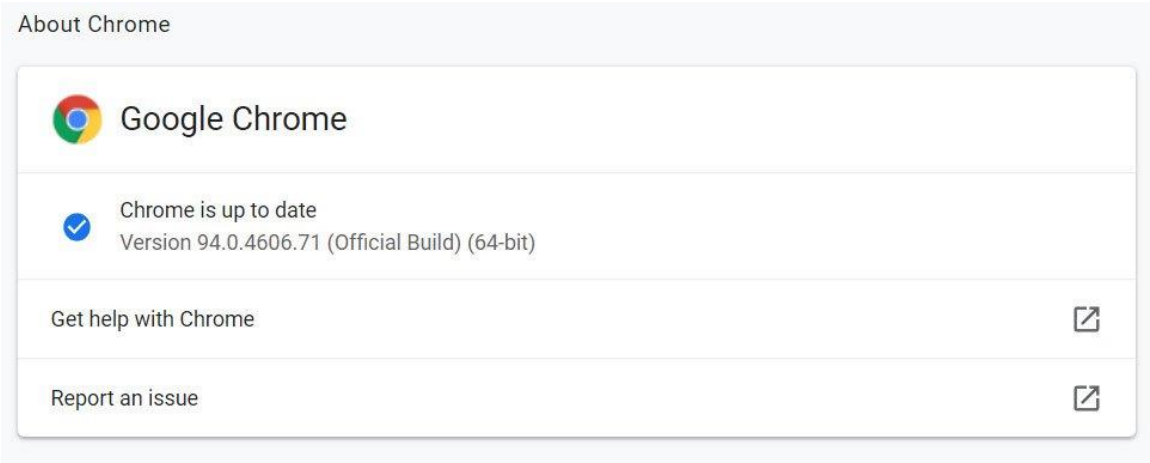
Google has released Chrome 94.0.4606.71 for Windows, Mac, and Linux, to fix two zero-day vulnerabilities that have been exploited by attackers.

"Google is aware the exploits for CVE-2021-37975 and CVE-2021-37976 exist in the wild," Google disclosed in the list of security fixes fixed in today's Google Chrome release.

Google has started rolling out Chrome 94.0.4606.71 to users worldwide in the Stable Desktop channel and should be available to all users within the coming days.

To install the update immediately, Google Chrome users can go to **Chrome menu** > **Help** > **About Google Chrome**, and the browser will begin performing the update.

In our tests, the new version of the browser was installed immediately using the above steps.



Chrome 94.0.4606.71 was installed immediately

Google Chrome will also check for available updates and install them the next time you launch the web browser.

Zero-day attacks' details not disclosed

While this Chrome release includes fixes for four security vulnerabilities, the two zero-days are concerning as they are known to have been exploited in the wild.

The first zero-day, tracked as **CVE-2021-37976**, is described as an "Information leak in core" and was assigned a Medium severity level. This vulnerability was discovered by

Clément Lecigne from Google TAG, with technical assistance from Sergei Glazunov and Mark Brand from Google Project Zero, on September 21st, 2021.

The second zero-day, tracked as **CVE-2021-37975**, is a High severity user after free bug in the Chrome V8 JavaScript engine. The researcher disclosed this vulnerability on September 24th and wished to remain anonymous.

Use after free bugs are commonly used to perform remote code execution or escape the browser's security sandbox.

At this time, there are no other details regarding how these zero-day vulnerabilities were used in attacks but may be released in future reports by Google TAG or Project Zero. [...]

Chrome users should perform a manual upgrade or restart their browser to install the latest version and prevent exploitation attempts.

Thirteenth zero-day fixed this year

With these two fixes, Google has patched 13 zero-day vulnerabilities in the Chrome web browser since the start of 2021. [...]

As Google is rushing out Chrome updates to fix zero-days as they are reported, it is always critical to install new browser updates as soon as they become available.

Source :https://www.bleepingcomputer.com/news/security/google-pushes-emergency-chrome-update-to-fix-two-zero-days/

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.