FRSECURE®

Under the Hood Recap:
Cyber Threat News and Recommendations

December 2020

News

Covid Sucks – and We're Getting PWND

A recent report published by our friends at Arctic Wolf states that since COVID has began we have observed:

- 35% of all attacks happen between the hours of 8PM and 8AM
    - Why? Because we are asleep. Attackers know the mean time to respond will increase during non-peak hours – increasing their likelihood of success.
- 64% Increase in Ransomware and Phishing attempts
    - With our remote workforce expanding significantly – that means the potential targets for attackers has increased as well. With a bigger "target pool" we are seeing a rather linear increase in targeting those employees and services.
- 429% Increase in account takeovers
    - As mentioned previously – as the attacker target list increases; attacks increase – and this statistic shows that the success level is also increasing.

Moral of the story? We were all faced with unexpected challenges this year, and had to respond rather rapidly, and often unprepared. With a surge in increase of remote workers, this also meant opening tools and applications to the internet for a much larger user base. It is incredibly important that all of those tools and applications are properly deployed – and you are deploying safeguards as needed to prevent system breach.

Full Arctic Wolf report can be found here:

https://arcticwolf.com/resources/analyst-reports/security-operations-annual-report

RDP Continues to be One of the Most Attacked Protocols

https://www.cisecurity.org/media-mention/center-for-internet-security-issues-new-remote-desktop-security-guide-based-on-cis-controls/

Currently there are around 3.5 Million publicly available RDP devices worldwide

Don't use publicly available RDP systems… If you must – follow these guidelines:

- Place RDP-enabled systems behind a Remote Desktop Gateway (RDG) or virtual private network (VPN). Require Multi-Factor!!
- Update and patch software that uses RDP
- Limit access to RDP by internet protocol (IP) and port
- Implement a AD group for those that require RDP

- Utilize unique accounts for remote access – Not your standard account and certainly not an admin account!
- Use complex, unique passwords for RDP-enabled accounts
- Implement a session lockout for RDP-enabled accounts
- Disconnect idle RDP sessions
- Secure Remote Desktop Session host

Ransomware Demands are Increasing—By a Lot

https://www.infosecurity-magazine.com/news/criminals-favor-ransomware-bec/

The average ransomware pay-outs for all businesses have grown from less than $10,000 in Q3 2018 to more than $178,000 per event by the end of Q2 2020. Large enterprises are making average ransomware payments of over $1m. BEC scams cost businesses more than $1.8bn in 2019.

Ransoms ROLL ON: Baltimore County, Huntsville Alabama

https://urgentcomm.com/2020/12/02/driven-by-ransomware-cyber-claims-rise-in-number-value/

Cyberattacks and security incidents have become the top business risk for companies, with the number of insurance claims rising 27% in the first nine months of 2020, according to a report released earlier this month by insurance company Allianz.

Exploit and IoC Deep Dive

FireEye Security Breach

https://www.zdnet.com/article/fireeye-one-of-the-worlds-largest-security-firms-discloses-security-breach/

We currently know very little about "how" this happened – but a nation state APT is suspected. At current time FireEye has employed MicroSoft as well as the FBI to assist in the investigation.

What we do know is why….

FireEye is a global player in information security with a rather large portfolio of clients and likely, a treasure trove of reconnaissance information regarding those clients. IE – having this wealth of information available will likely save attackers a significant amount of time as they posture for future attacks.

We also know that FireEye has developed a very impressive catalogue of proprietary offensive security tools. These were confirmed as being stolen during the attack.

What can we expect? That attackers will use the information obtained from this attack, as well as the tools obtained from the attack in future campaigns.

What can you do? If you are a FireEye customer – engage them immediately and determine if any of your previous records were involved in the breach. This is rather important, as mentioned before, because this data can be used against you in future attacks.

Also – implement blocks for all of stolen FireEye tools within your security stack. FireEye has released a GitHub that includes signatures for Yara, Snort, and ClamAV. If you are using any Cisco AMP, umbrella, or FIrePower IPS – these signatures should be applied in your products. Review your cisco appliances and confirm. For all the others – I have developed a human-readable extract of the IoC's that you can use to implement in your own security stack. My IoC list was extracted from this data but was filtered to include the Name and MD5 hash of the tool – this will allow you to easily transfer into your EDR, and end-point tools.

https://github.com/fireeye/red_team_tool_countermeasures

APT10 Cicada is targeting Zero-Logon

Cve 2020-1472

https://www.bankinfosecurity.com/chinese-hackers-exploiting-zerologon-flaw-for-cyberespionage-a-15406

Zero-Logon, also known as CVE-2020-1472, is currently being targeted in the killchain for APT10 Cicada. For a full analysis of the Zero-Logon exploit, go check out our recently published article:

https://frsecure.com/blog/cve-2020-1472/

A high-level overview of the common attack pattern is as follows:

1. Use the ZeroLogon attack to authenticate as a domain controller to a domain controller
2. Set the domain controller's machine password to blank
3. Authenticate properly with the domain controller's account
4. Perform a DCSync attack to extract password hashes from Active Directory
5. (optional) Set the domain controller's machine password back to its original value to prevent obvious issues and cover the attacker's tracks

This can all be performed in seconds.

What can you do to prevent this? Patch. An update was released by Microsoft in August of this year. Detection methods outside of this are rather difficult – but for details refer to the FRSecure article linked above.

This isn't the only exploit utilized by Cicada – so let's talk a little bit more about the TTP's utilized by this advanced persistent threat. They LOVE living of the land techniques, just as most sophisticated attackers. For those that don't know what this means it's rather simple – abusing legitimate tools that exist in most environments to execute malicious activity. They also love DLL Sideloading – which is a technique to replace code of a legitimate DLL with their malicious payload – obfuscating the payload from detection. They have also recently been observed a new backdoor exploit – Backdoor.Hartip. Below is a list of other tools and techniques utilized by the group. Also, see our attached Cicada IoC list for all known hashes of their malicious tools as well as IP's that have been identified in their kill-chain. We recommend blocking all of these within your security stack.

- **Certutil** – Decode information, download files, install browser certificates
  - Built in Microsoft Command
  - Utilized to decode information, download files and install browser certificates
  - Certutil.exe is a command-line program, installed as part of Certificate Services. You can use certutil.exe to dump and display certification authority (CA) configuration information, configure Certificate Services, backup and restore CA components, and verify certificates, key pairs, and certificate chains.
- **Adfind**
  - Utilized to Perform Active Directory queries
  - http://www.joeware.net/freetools/tools/adfind/
  - Command line Active Directory query tool. Mixture of ldapsearch, search.vbs, ldp, dsquery, and dsget tools with a ton of other cool features thrown in for good measure. This tool preceded dsquery/dsget/etc by years though I did adopt some of the useful stuff from those tools.
- **Csvde**
  - Built in Microsoft tool
  - Utilized to extract Active Directory files and data
- **Ntdsutil**
  - **Built in Microsoft Tool**
  - Ntdsutil.exe is a command-line tool for accessing and managing a Windows Active Directory (AD) database. Microsoft recommends that Ntdsutil only be used by experienced administrators and requires that the tool be used from an elevated command prompt
  - Utilized for Credential Dumping
- **WMIExec**
  - Build in Microsoft Tool
  - Remote command execution and lateral movement
- **PowerShell** –
  - Built in Microsoft tool
  - Used for malicious code execution
- **DLL SideLoading** – DLL side-loading occurs when attackers are able to replace a legitimate library with a malicious one, allowing them to load malware into legitimate processes. Attackers use DLL side-loading to try and hide their activity by making it look legitimate, and it also helps them avoid detection by security software

- **QuasarRAT** – an open-source backdoor used by Cicada in the past
- **Backdoor.Hartip –** Recently identified backdoor used by Cicada.

- **Known to exfil data** – typically archive in .RAR before stealing
- **Legitimate cloud hosting service for exfil** – Google, AWS

Last Patch Tuesday of the Year—And It's a Doozy

9 Critical updates included. No current PoC for exploits, but I expect they are coming very shortly. Also, of note – a high risk for an Office RCE was included. This is important and we ask you consider the statistics we shared regarding phishing earlier i the report. Many phishing campaigns utilize remote code exploits within the office suite to execute their payload. Further – we see many ransomware attacks that originate from a payload delivered via these phishing campaigns. Therefore – it's critically important to get these patches rolled out to lower your likelihood of a compromise.

It is also being reported that Microsoft quietly resolved a "zero-click" vulnerability within Teams. This vulnerability would allow an attacker to deliver a specially crafted message to a victim that would permit remote code execution, or payload delivery. Again – the payload required no interaction from the victim – they simply had to look at the message. Full details of this payload can be reviewed in Oskar Vegeris github page:

https://github.com/oskarsve/ms-teams-rce/blob/main/README.md

Vergeris has also stated that this bug is one of five that have been reported to Microsoft and it is unclear if the others have been resolved.

Quick Hits and Other Things to Know

VMWare – Unrestricted access to Underlying Machine OS

CVE 2020 4006

What you need to know:

A bug exists in the administrative configurator of VMWare on port 8443 that permits an attacker the ability to execute unrestricted commands on virtual machines underlying OS. To successfully exploit this an attacker would have to have access to the console and possess the configurator password. This is usually created on setup of the implementation.

What do do?

- Patch immediately!
- LockDown access to the configurator port – only permit required IPs.
- Ensure the configurator password is complex and properly secured.

https://www.vmware.com/security/advisories/VMSA-2020-0027.html

WebLogic RCE

CVE-2020-14882

A vulnerability exists in Oracle WebLogic Server console component that allows remote code execution. This can be used to deploy a malicious payload or backdoor on affected systems. The exploit does not require authentication.

This is currently being exploited in the wild. There are 3100 publicly available vulnerable systems worldwide.

What to do?

Patch your systems immediately. f you identify that you have an unpatched system that is available on the internet – a forensic investigation should be completed to determine if the system was previously exploited.

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14882

Another day another Drupal bug

CVE-2020-28948 and CVE-2020-28949

Vulnerabilities have been identified in the open-source PEAR Archive_Tar library which is utilized by Drupal to handle TAR files in PHP that permits arbitrary code execution.

What to do?

This is only applicable if your Drupal configuration allows .tar; .tar.gz; bz2; or .tlz files to be uploaded. If this service is not required – ensure it is not enabled in your configuration.

Drupal has also released an out-of-band patch, it is recommended to apply these at your earliest.

https://nvd.nist.gov/vuln/detail/CVE-2020-28949

iPhone – Zero-Click Exploit

It is my hope that most will not be affected by this vulnerability as only IOS version 13.5 is affected. If you are properly updating your iPhone, you are properly secured.

The vulnerability is known as a zero-click exploit as it required no interaction from the victim to successfully exploit. The vulnerability permits an attacker to harvest data by exploiting a weakness in the iPhone Wi-Fi and airdrop functionality. If you have a few minutes – watch the video in the link below – it's rather impressive and a warning that our pocket computers aren't as secure as many often believe.

What you should do?

- Ensure your devices are always updated to the latest OS build.
- Don't allow your phone to auto-connect to Wi-Fi networks.
- Disable Wi-Fi and AirDrop service when traveling or not in use.

https://arstechnica.com/gadgets/2020/12/iphone-zero-click-wi-fi-exploit-is-one-of-the-most-breathtaking-hacks-ever/

Contact

If you run into issues, concerns, or questions with any of the topics listed above, please do not hesitate to reach out to the FRSecure team.