Security Bulletin

(Threat Advisories & Trending News)

14th December, 2018

Table of Contents

1. Summary

This advisory captures some of the critical threats, vulnerabilities and key cyber security headlines in news during the week that might require immediate attention.
The specific **critical** threats / vulnerabilities are:

Vulnerability Details

- Zero-Day Bug Fixed by Microsoft
- Adobe Acrobat Reader DC text field remote code execution vulnerability

Malware Campaign

- Satan Ransomware Variant – Impacts Linux and Windows
- Shamoon 3 Targets Oil and Gas Organization
- Dear Joohn: The Sofacy Group's Global Campaign

Popular Security News

- Microsoft, PayPal and Google Top the Brands Hit by Phishing
- Claroty Adds New Capabilities to Industrial Security Platform
- Organizations Still Slow to Detect Breaches: CrowdStrike
- Apache Misconfig Leaks Data on 120 Million Brazilians

2. Vulnerability Details

Zero-Day Bug Fixed by Microsoft

Released date: 11th December, 2018
CVE-Detials: CVE-2018-8611, CVE-2018-8517, CVE-2018-8634
Affected Products: Windows

Description:
The vulnerability (CVE-2018-8611) is an elevation-of-privilege (EoP) bug that affects Windows 7 through Server 2019. It has a CVSS rating of seven, classifying it as a high-severity flaw.
CVE-2018-8517 is a flaw in .NET framework having denial-of-service issue.
CVE-2018-8634 is a remote code execution bug in Microsoft's text-to-speech engine.

Attack Scenario:

- The attacker would first have to log onto the system then run a specially crafted application to take control of the affected system.
- A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to the .NET Framework application

Impact:
An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user right.

Mitigation:
Microsoft has issued patches for the vulnerability.

Adobe Acrobat Reader DC text field remote code execution vulnerability

Released date: 11th December, 2018
CVE-Detials: CVE-2018-19716
Affected Products: Adobe Acrobat Reader DC 2019.8.20071

Description:
Vulnerability is present in Adobe Acrobat Reader. Adobe Acrobat Reader supports embedded JavaScript in PDFs to allow for more user interaction. However, this gives the attacker the ability to precisely control memory layout, and it poses an additional attack surface.

Attack Scenario:
If the attacker tricks the user into opening a PDF with two specific lines of JavaScript code, it will trigger an incorrect integer size promotion, leading to heap corruption. It's possible to corrupt the heap to the point that the attacker could arbitrarily execute code on the victim's machine.

Impact:
On successful exploitation the attacker can perform remote code execution and use the compromise machine for other malicious activities.

Mitigation:
Adobe has issued patches for the vulnerability.

3. Malware Campaign

Satan Ransomware Variant – Impacts Linux and Windows

Date: 11th December, 2018

Description:
NSFOCUS discovered that financial customers are getting infected with a worm virus FT.exe that could affect both Linux and Windows platforms. Like the ransomware Satan, the virus spreads itself by exploiting multiple application vulnerabilities. However, this virus, after breaking into the system, does not do anything obviously damaging, but only spreads itself. Its a cross-platform ransomware, which was believed to be a variant of FT.exe with the capability of dropping Monero miners and ransomware. This variant can propagate itself via Linux and Windows platforms like a worm. In addition, it encrypts local files and appends .lucky to their names besides dropping a ransom file with the name of "_How_To_Decrypt_My_File_".

Indicators of Compromise:
IP:

- 111.90.158.225
- 107.179.65.195
- 23.247.83.135
- 111.90.158.224

HTTP Request:

- http://111.90.158.225/wversion
- http://107.179.65.195/wversion
- http://23.247.83.135/wversion
- http://111.90.158.224/wversion

Vulnerabilities list:

- JBoss deserialization vulnerability
- JBoss default configuration vulnerability (CVE-2010-0738)
- Tomcat arbitrary file upload vulnerability (CVE-2017-12615)
- Tomcat web admin console backstage weak password brute-force attack
- WebLogic arbitrary file upload vulnerability (CVE-2018-2894)
- WebLogic WLS component vulnerability (CVE-2017-10271)
- Windows SMB remote code execution vulnerability (MS17-010)
- Apache Struts 2 remote code execution vulnerability (S2-045)
- Apache Struts 2 remote code execution vulnerability (S2-057)
- Spring Data Commons remote code execution vulnerability (CVE-2018-1273)

Linux Detection:

- **ps -ef | grep loop** and **ps -ef | grep conn** commands to check whether loop and conn processes are running.
- **find / -name ".loop", find / -name ".conn", and find / -name ".hash"** commands to search for .loop, .conn, and .hash files across directories.
- **crontab -l** command to check whether .loop is included in auto startup items.
- Check for the .lucky extension.
- Check whether there is the **/etc/rc6.d/S20loop** file.

Windows Detection:

- Check the **C:\ directory for fast.exe** or **_How_To_Decrypt_My_File_.**
- Check the **C:\Program Files\Common Files\System** directory for **conn.exe and srv.exe**.
- Check the **C:\user\all users or C:\ProgramData** directory for the **EternalBlue** toolkit.
- Check whether **blue.exe, fast.exe, star.exe, srv.exe, conn.exe, cpt, and mmkt.exe** processes are running in the system.
- Check whether an abnormal registry key/value exists to find out the presence of the logs service: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Logs Service**.

Impact:

The Satan virus family propagates itself by exploiting 10 common vulnerabilities listed below. Satan scans for these vulnerabilities on the Linux platform by means of internal IP address traversal and port listing, and on the Windows platform by means of IP address and port listing. Version 10- the virus of this version, after breaking into the system, does not do anything obviously damaging, but only spreads itself. Version 13- This version adds a ransomware module, which encrypts local files and appends .lucky to their names before dropping the ransom file with the name of "_How_To_Decrypt_My_File_".

Mitigation:

- Block the IOCs
- Upgrade Apache Struts 2 to the latest version that has fixed S2-045, S2-046, and S2-057 vulnerabilities.
- Upgrade JBoss to the latest version that has fixed CVE-2013-4810 and CVE-2010-0738 vulnerabilities.
- Upgrade Tomcat to fix the arbitrary file upload vulnerability (CVE-2017-12615).
- Upgrade WebLogic to fix the arbitrary file upload vulnerability (CVE-2018-2894) and WLS component vulnerability (CVE-2017-10271).
- Patch the operating system to fix the MS17-010 vulnerability or disable the SMB service if it is unnecessary.
- Increase the complexity of host account passwords and set the password change cycle to a short period. Besides, avoid using common passwords or passwords with logical meanings.
- Change the default user name of system administrator to avoid the use of common ones such as admin, administrator, and test.

- Install antivirus software with self-protection to avoid being shut down or terminated by hackers, and keep the virus database up to date.
- Step up training on employee security awareness. Do not open emails from unknown senders or run programs from unidentifiable sources.
- Back up mission-critical business data regularly to avoid issues incurred by data corruption and loss.
- Use VLANs or port isolation to separate different business networks to prevent viruses from spreading across network segments.
- Keep track of vulnerability alerts, for example, by following the official WeChat account of NSFOCUS for security alerts, so as to be able to fix critical vulnerabilities in time.

Removal of malware:

Linux

- Get the machine offline and isolate it from other machines on the same network to avoid a secondary infection during trojan removal.
- Check crontab and local files and delete startup information of the Satan virus (if any).
- Use kill -9 pid to terminate .loop, .conn32/64, and .cry32/64
- Check where the /etc/rc6.d/S20loop directory points and delete the sample program files from this directory, including .loop, .conn32/64, and .cry32/64 before deleting /etc/rc6.d/S20loop.
- Change the password of the SSH service on the operating system to a strong one.

Removal of the Trojan from Windows

- Get the machine offline and isolate it from other machines on the same network to avoid a secondary infection during trojan removal.
- As the trojan incorporates the weak password scanning capability and the password capture tool mmkt.exe, it is necessary to change the system password to avoid a secondary infection during trojan removal.
- Terminate exe, fast.exe, star.exe, srv.exe, conn.exe, mmkt.exe, and cpt.exe processes.
- Delete exe, srv.exe, and cpt.exe from C:\Program Files\Common Files\System.
- Delete the EternalBlue toolkit from C:\user\all users or C:\ProgramData (note the write time to avoid mistakenly deleting normal system files).
- Delete the registry key/value created by the trojan: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Logs Service.
- Install the operating system patch specially developed to address the MS17-010 vulnerability (EternalBlue exploit).

Shamoon 3 Targets Oil and Gas Organization

Date: 13th December, 2018

Description:
On December 10, a new variant of the Disttrack malware was submitted to VirusTotal (SHA256:c3ab58b3154e5f5101ba74fccfd27a9ab445e41262cdf47e8cc3be7416a5904f) that shares a considerable amount of code with the Disttrack malware used in the Shamoon 2 attacks in 2016 and 2017Unit42 researchers have further analysed the sample. Saipem disclosed that they were attacked. However, that functionality was missing from this sample. Unlike past Shamoon attacks, this particular Disttrack wiper would not overwrite files with an image. Instead it would overwrite the MBR, partitions, and files on the system with randomly generated data. The attack caused infrastructure and data availability issues, forcing the organization to carry out restoration activities.

Indicators of Compromise:

Hashes:

- c3ab58b3154e5f5101ba74fccfd27a9ab445e41262cdf47e8cc3be7416a5904f
- 0975eb436fb4adb9077c8e99ea6d34746807bc83a228b17d321d14dfbbe80b03
- 0694bdf9f08e4f4a09d13b7b5a68c0148ceb3fcc79442f4db2aa19dd23681afe
- 391e7b90bf3f0bfeb2c2602cc65aa6be4dd1c01374b89c4a48425f2d22fe231c
- 6985ef5809d0789eeff623cd2436534b818fd2843f09fa2de2b4a6e2c0e1a879
- ccb1209122085bed5bded3f923835a65d3cc1071f7e4ad52bc5cf42057dd2150
- dab3308ab60d0d8acb3611bf364e81b63cfb6b4c1783864ebc515297e2297589
- bc4513e1ea20e11d00cfc6ce899836e4f18e4b5f5beee52e0ea9942adb78fc70

Base64 Key:

- 2q9BQGHGVktPVIMZ6Nx17Njp4B5mHgj51hbybNInRWsNIWniq6hOYvf5CksMXvPOyl/3dYKDn7ymSGlK0+l5KA8YC8dzkkAwmn0nbBO97HgjJKJyL9DoiYKsO2M+A44NgOI89FIsWjcex9oEWzOo6VvxJ69HBvg+L4FExlbd8ZfvGewxgPgl98lqVGj14y5OBFIHTdvfxnnq/cTR55TgQdVDFUJHd2ljyzDl3LKPSUxT9sIE1aS7EA==
- U3JGgjNUDzWJEpOxzuwHjOijgav56cZatHh98dLbazGIBe7UMOcvdyCvU5/8mH1n7jUcMSIPFmqr7M671h5jradiKMn9M1sBdAmKSZUnXhz6FQKcvzkOee6EKEQZdKABTKX4mW+0arvZG70YhczUhI2ywcEcx+5tU6/aeQoX6ABoiP3wLsSsRatGwqR89fMir6S2Z7Lf5YW3i0a/2vCxwjK9r/zO5FXJBXsV1QRJ8F27t8pmYYFNiaN4OaN+7Gu7lf8=
- cb5F91PLTu1hN8oPgG2a6AQiJkphsXAmWFarsUoYEFo/BNgxF8Rj/hdzHxW/k/fLCZboSJRLnr9OH578IJyiSSdvz3uUaNA/vycy7ZJaZ8Vf36i0L8fF9GYY4/glZt570dbuT8N7N6DFqIltGLAt87fZnUH07RlfqtsVfITXGlhJtxu7bBgB46gH74Y+WNy16u9BS8mdh+S8jqToZrob7o4wI2CUcoaf17mZ7P2SIVL+X5GVls6OrDA3/t50GX3t6wH4DTR7IHhoonQPA5rmKWxS6gcp
- heocXOK4rDmQg4LRfiURI9wSOuSMwe0e69NfEpZLmyNixiUGYdEtpx/ZG3rMRN7GZlJ1/crQTz5Bf6W0xgkyYCwzD247FolCGA0EE5U/Oun5qlDd1u1CA+fee7cG

Files installed:

- MaintenaceSrv32.exe
- MaintenaceSrv64.exe

Dropper File Name: Dropper randomly chooses the name when installing the communication

- netnbdrve
- prnod802
- netrndiscnt
- netrtl42l
- mdmadccnt
- prnca00
- bth2bht_ibv32
- cxfalcon_ibL32
- mdmsupr30
- digitalmediadevicectl
- mdmetech2dmv
- netb57vxx
- winwsdprint
- prnkwy005
- composite005
- mdmar1_ibv32
- prnle444
- kscaptur_ibv32
- mdmzyxlga
- usbvideob
- input_ibv48
- prnok002_ibv
- averfx2swtvZ
- wpdmtp_ibv32
- mdmti_ibv32
- printupg_ibv32
- wiabr788

Wiper module name: The wiper module will have one of the following filenames

- _wialx002
- __wiaca00a
- tsprint_ibv
- acpipmi2z
- prnlx00ctl
- prngt6_4
- arcx6u0
- _tdibth

- prncaz90x
- mdmgcs_8
- mdmusrk1g5
- netbxndxlg2
- prnsv0_56
- af0038bdax
- averfix2h826d_noaverir
- megasasop
- hidirkbdmvs2
- vsmxraid
- mdamx_5560
- wiacnt7001

Impact:
The sample submitted to VirusTotal is a Disttrack dropper according to Unit42 researchers, which is responsible for installing a communications and wiper module to the system. The dropper is also responsible for spreading to other systems on the same local network, which it accomplishes by attempting to log into other systems on the network remotely using previously stolen usernames and passwords. Unfortunately, this particular sample does not contain any domains, usernames, or passwords to perform this spreading functionality, so this sample would only run on the system in which it was specifically executed.

Mitigation:
- Block the IOCs
- The tool does not have the capability to spread to other systems on the local network. Instead it would have to be loaded onto and executed on the system that the actors intend to wipe.

Dear Joohn: The Sofacy Group's Global Campaign

Date: 12th December, 2018

Description:
Unit42 researchers have observed a new global campaign conducted by Sofacy group (AKA Fancy Bear, APT28, STRONTIUM, Pawn Storm, Sednit). The Sofacy group has persistently attacked various government and private organizations around the world from mid-October 2018 through mid-November 2018. The majority of targets were NATO-aligned nation states, although several former USSR nation states were also targeted. The attacks primarily deployed variants of the Zebrocy tool. The attack vector for all of these attacks appears to be via spear-phishing, using email accounts registered to legitimate email providers instead of spoofed email addresses or previously compromised accounts. The account names visually look similar to legitimate government organization names or other trusted third-party entities. The delivery documents were functionally all the similar, using the remote template function in Microsoft Word to retrieve a malicious macro from the first stage C2 and ultimately loading and executing an initial payload. The majority of delivery documents contain a generic lure image requesting the victim enable macros with no additional content, the adversaries seemingly relying solely on lure filenames to entice victims to launch the malicious document.

Indicators Of Compromise:

Delivery Hashes:

- 2cfc4b3686511f959f14889d26d3d9a0d06e27ee2bb54c9afb1ada6b8205c55f
- c20e5d56b35992fe74e92aebb09c40a9ec4f3d9b3c2a01efbe761fa7921dd97f
- abfc14f7f708f662046bfcad81a719c71a35a8dc5aa111407c2c93496e52db74
- 40318f3593bca859673827b88d65c5d2f0d80a76948be936a60bda67dff27be9
- 5749eb9d7b8afa278be24a4db66f122aeb323eaa73a9c9e52d77ac3952da5e7d
- af77e845f1b0a3ae32cb5cfa53ff22cc9dae883f05200e18ad8e10d7a8106392
- 34bdb5b364358a07f598da4d26b30bac37e139a7dc2b9914debb3a16311f3ded
- 79bd5f34867229176869572a027bd601bd8c0bc3f56d37443d403a6d1819a7e5
- 77ff53211bd994293400cb3f93e3d3df6754d8d477cb76f52221704adebad83a

Remote Template Hashes:

- f1e2bceae81ccd54777f7862c616f22b581b47e0dda5cb02d0a722168ef194a5
- 86bb3b00bcd4878b081e4e4f126bba321b81a17e544d54377a0f590f95209e46
- 2da5a388b891e42df4ed62cffbc167db2021e2441e6075d651ecc1d0ffd32ec8
- 0d7b945b9c912d205974f44e3742c696b5038c2120ed4775710ed6d51fbc58ef
- fc69fb278e12fc7f9c49a020eff9f84c58b71e680a9e18f78d4e6540693f557d
- ed8f52cdfc5f4c4be95a6b2e935661e00b50324bee5fe8974599743ccfd8daba
- b9f3af84a69cd39e2e10a86207f8612dd2839873c5839af533ffbc45fc56f809

Remote Template URLs:

- hxxp://188.241.58[.]170/live/owa/office.dotm
- hxxp://185.203.118[.]198/documents/Note_template.dotm
- hxxp://185.203.118[.]198/documents/Note_template.dotm
- hxxp://145.249.105[.]165/doc/temp/release.dotm
- hxxp://145.249.105[.]165/messages/content/message_template.dotm
- hxxp://188.241.58[.]170/version/in/documents.dotm
- hxxp://109.248.148[.]42/officeDocument/2006/relationships/templates.dotm
- hxxp://109.248.148[.]42/office/thememl/2012/main/attachedTemplate.dotm
- hxxp://109.248.148[.]42/office/thememl/2012/main/attachedTemplate.dotm

Zebrocy Hashes:

- 5173721f3054b92e6c0ff2a6a80e4741aa3639bc1906d8b615c3b014a7a1a8d7
- 61a1f3b4fb4dbd2877c91e81db4b1af8395547eab199bf920e9dd11a1127221e
- 6ad3eb8b5622145a70bec67b3d14868a1c13864864afd651fe70689c95b1399a
- 9a0f00469d67bdb60f542fabb42e8d3a90c214b82f021ac6719c7f30e69ff0b9
- b41480d685a961ed033b932d9c363c2a08ad60af1d2b46d4f78b5469dc5d58e3
- c91843a69dcf3fdad0dac1b2f0139d1bb072787a1cfcf7b6e34a96bc3c081d65
- e5aece694d740ebcb107921e890cccc5d7e8f42471f1c4ce108ecb5170ea1e92

Zebrocy C2 URLs:

- hxxp://188.241.58[.]170/local/s3/filters.php
- hxxp://185.203.118[.]198/en_action_device/center_correct_customer/drivers-i7-x86.php
- hxxp://145.249.105[.]165/resource-store/stockroom-center-service/check.php
- hxxp://109.248.148[.]42/agr-enum/progress-inform/cube.php

Cannon Hashes:

- 861b6bc1f9869017c48930af5848930dd037fb70fc506d8a7e43e1a0dbd1e8cb
- 4405cfbf28e0dfafa9ea292e494f385592383d2476a9c49d12596b8d22a63c47
- 174effcdeec0b84c67d7dc23351418f6fa4825550d595344214cc746f1a01c1a
- a23261e2b693750a7009569df96ec4cf61e57acc9424c98d6fe1087ff8c659ce
- 651d5aab82e53711563ce074c047cbaa0703931673fa3ad20933d6a63c5c3b12
- 68df0f924ce79765573156eabffee3a7bb0fa972d2b67d12dd91dea3ec255d24
- 61a1f3b4fb4dbd2877c91e81db4b1af8395547eab199bf920e9dd11a1127221e
- 5a02d4e5f6d6a89ad41554295114506540f0876e7288464e4a70c9ba51d24f12
- d06be83a408f4796616b1c446e3637009d7691c131d121eb165c55bdd5ba50b4
- 78adc8e5e4e86146317420fa3b2274c9805f6942c9973963467479cb1bbd4ead
- 054c5aa73d6b6d293170785a82453446429c0efc742df75979b760682ac3026b
- cac630c11c4bf6363c067fbf7741eae0ec70238d9c5e60d41f3ed8f65b56c1d1
- ecc5805898e037c2ef9bc52ea6c6e59b537984f84c3d680c8436c6a38bdecdf4
- 215f7c08c2e3ef5835c7ebc9a329b04b8d5215773b7ebfc9fd755d93451ce1ae

Cannon Related Emails

- sym777.g[at]post.cz
- kae.mezhnosh[at]post.cz
- vebek.morozh30[at]post.cz
- g0r7tsa45s[at]post.cz
- marvel.polezha[at]post.cz
- sahro.bella7[at]post.cz
- trala.cosh2[at]post.cz
- Bishtr.cam47[at]post.cz
- Lobrek.chizh[at]post.cz
- Cervot.woprov[at]post.cz
- heatlth500[at]ambcomission[.]com
- trash023[at]ambcomission[.]com
- trasler22[at]ambcomission[.]com
- rishit333[at]ambcomission[.]com
- tomasso25[at]ambcomission[.]com
- kevin30[at]ambcomission[.]com

Attached File Names:

- 1500029.docx
- Passport.docx
- DN_325_170428_DEA Basic Narcotics Investigation Course invitation.docx
- 2018_10_13_17_15_21.docx
- crash list(Lion Air Boeing 737).docx
- Заявление.docx
- Rocket attacks on Israel.docx
- 201811131257.docx
- Brexit 15.11.2018.docx
- DIP 89 OIC Condemns 14 Nov Attacks.docx
- 15.11 attacks.docx

Impact:
The targets included a foreign affairs organization in North America, foreign affairs organizations in Europe, as well as government entities in former USSR states. We also discovered evidence of possible targeting of local law enforcement agencies around the world, covering North America, Australia, and Europe. As the campaign is covering the large part, hence the impact will be more.

Mitigation:

- Block the IOCs
- Disable all macros by default and only run macros vetted as trustworthy.

4. Popular Security News

Microsoft, PayPal and Google Top the Brands Hit by Phishing

Date: 12th December, 2018
Source: https://www.infosecurity-magazine.com/news/microsoft-paypal-google-top-the/

Email phishing continues to be the most common method of attack, and according to new research from Comodo Cybersecurity Microsoft, PayPal and Google are the top three brands most targeted by phishing.

In its Global Threat Report 2018 Q3, researchers in Comodo's threat research lab found that phishing represents one of every 100 emails received by enterprises, with 19% of those attacks targeting Microsoft, followed by 17% targeting PayPal and 9.7% going after Google.

According to the report, 63% of the emails a business receives are clean, while 24% are spam, and only 1.3% of business emails are phishing attempts. Of those, there were three subject lines that were used with great frequency.

In 40% of the phishing emails examined, the subject line was related to PayPal and read, "Your account will be locked." Another 10% of phishing emails targeted FedEx and read "Info," while the third-most popular headline, "August Azure Newsletter," appeared in 8% of the phishing emails and targeted Microsoft.

While malicious attachments remain the top method of infection, phishing URLs are also gaining popularity and represent 40% of the total phishing emails analyzed. In one example, researchers discovered an email claiming to be a survey of that Azure newsletter. The message contained what appeared to be an authentic URL and Microsoft logo, which made it very difficult for users to determine whether it was legitimate. If users clicked on the link, they were delivered to a malware-laden web page, where they were covertly infected.

The report also found that there was a surge in malware deployment in advance of major national elections across the globe, as well as correlations of malware detection both prior to and immediately following geopolitical crises.

"These correlations clearly stand out in the data, beyond the realm of coincidence," said VP of Comodo's cybersecurity threat research labs Fatih Orhan. "It is inescapable that state-actors today employ malware and other cyber-threats as both extensions of soft power and outright military weapons, as do their lesser-resourced adversaries in asymmetric response."

Claroty Adds New Capabilities to Industrial Security Platform

Date: 12th December, 2018
Source: https://www.securityweek.com/claroty-adds-new-capabilities-industrial-security-platform

Industrial cybersecurity firm Claroty on Tuesday announced significant enhancements to its threat detection product, along with technology integrations with several cybersecurity, network infrastructure and industrial automation providers.

Claroty provides an ICS security platform that includes real-time threat detection, continuous vulnerability monitoring, and secure remote access capabilities.

The latest release of the company's Continuous Threat Detection product introduces virtual zones and OT network segmentation. This helps organizations automate the creation of virtual zones based on how their industrial automation systems are configured and how they are communicating. The new functionality also helps enforce network segmentation through firewall and network access control (NAC) policies.

Another enhancement is multispectral data acquisition, which provides organizations nearly 100% visibility into the assets on their OT network, including what those assets are, what they do, how they are configured, and how they communicate.

Claroty announced that its products can be integrated with technology from several other vendors, including network infrastructure providers (Cisco, Siemens, Palo Alto, CheckPoint), network access control providers (ForeScout, Cisco), SIEM and analytics providers (Splunk, IBM QRadar, RSA), and endpoint detection and remediation providers (TripWire).

"These enhancements to the Claroty Platform fill critical gaps in the industrial cybersecurity market, where industrial enterprises and critical infrastructure providers have been increasingly impacted by cyberattacks targeting OT networks and broad-based attacks which "spillover" from IT networks into the operational environment," explained Patrick McBride, chief marketing officer at Claroty.

"As our customer base continues to grow very rapidly, we are listening to our customers, working alongside them and developing the innovative capabilities they need to safely, cost-effectively and rapidly develop a robust cybersecurity capability for their most critical, revenue generating systems," McBride added.

Claroty has raised a total of $93 million, including $60 million in a Series B funding round in June.

Organizations Still Slow to Detect Breaches: CrowdStrike

Date: 11th December, 2018

Source: https://www.securityweek.com/organizations-still-slow-detect-breaches-crowdstrike

Organizations are getting better at detecting intrusions on their own, but it still takes them a long time to do it, according to a new report published on Tuesday by endpoint security firm CrowdStrike. According to the 2018 CrowdStrike Services Cyber Intrusion Casebook, which is based on the analysis of over 200 major security incidents, 75% of organizations that used CrowdStrike's incident response services in 2018 managed to internally detect a breach, up from 68% in the previous year.

CrowdStrike believes organizations should be able to detect a threat within one minute, investigate it in ten minutes, and remediate it within 60 minutes – the company calls this the 1-10-60 rule. As for attack objectives, CrowdStrike says nearly half of the incidents analyzed by its experts were financially motivated. The second most common attack objective was intellectual property theft (30%), followed by theft of personal information (10%), ransomware (7%), cryptocurrency mining (3%), destruction (2%), and corporate espionage (1%).

Social engineering, phishing and spear-phishing were the attack vector in roughly one-third of cases, up from 11% in the previous year. The biggest single vector remains web server attacks, accounting for nearly 20% of the total. CrowdStrike has highlighted several important attack trends. The company says malicious actors have continued to come up with creative tactics and techniques. For example, experts uncovered cases where the attackers had been using remote access tools that provided them the ability not only to read their victims' emails, but also to watch the email being written and sent in real time.

The company's investigations also included cases where adversaries re-entered an organization's network shortly after another vendor's incident response team had been called in by the victim, and even cases where the attacker was still present on the network even after an incident response team believed that the threat was removed. Another major problem highlighted by CrowdStrike is that attackers continue to masquerade as legitimate users. State-sponsored actors often rely on stolen credentials for email and VPN access, while profit-driven cybercriminals use credential stuffing and business email compromise (BEC) tactics.

"In addition to detailing an uptick in social engineering, phishing and business email compromise attacks, we also established that many adversaries use commodity malware to launch destructive attacks and continue to leverage living-off-the-land techniques to stay undetected. To combat these challenges, CrowdStrike continues to advocate for faster and more effective detection and response, including the 1-10-60 rule that helps businesses lay the essential groundwork to defeat adversaries. The Services Casebook can be used as a critical guide for Corporate Boards and C-suites looking to safeguard their most valuable data," Etheridge added.

Apache Misconfig Leaks Data on 120 Million Brazilians

Date: 13th December, 2018
Source: https://www.infosecurity-magazine.com/news/apache-misconfig-leaks-data-120/

The identity numbers of 120 million Brazilians have been found publicly exposed on the internet after yet another IT misconfiguration.

The data relates to Cadastro de Pessoas Físicas (CPFs): ID numbers issued by Brazil's central bank to all citizens and tax-paying residents. The size of the leak represents data on over half the population of South America's biggest country. Researchers at InfoArmor's Advanced Threat Intelligence Team found the database exposed on an Apache web server in March, after a simple internet search.

"Upon closer examination of the server that was discovered by InfoArmor's researchers, it was found that someone had renamed the 'index.html' to 'index.html_bkp,' revealing the directory's contents to the world. Anyone who knew the filename or navigated to it would have unfettered access to all the folders and files within," its report explained.

"Two simple security measures could have prevented this: not renaming the main index.html file or prohibiting access through .htaccess configuration. Neither of these basic cybersecurity measures were in place." Only weeks later, after the firm unsuccessfully tried to contact the SQL host, did the issue get fixed.

"What was originally misconfigured to be accessible by IP address was reconfigured as a functional website with an authenticated alibabaconsultas.com domain that redirected to its login panel," it explained. "Although InfoArmor cannot be sure that alibabaconsultas.com was responsible for the leak, it appears they were somehow involved, likely in a hosting-as-a-service function."

The security firm warned that "it is safe to assume" either a nation state or cybercrime group now has the leaked information. Ilia Kolochenko, CEO of High-Tech Bridge, said a thorough investigation is required by the Brazilian government.

"The major question here is how did this highly sensitive and confidential data go online on a third-party server in a flagrant violation of all possible security, compliance and privacy fundamentals? Who else has access to this data and its copies?" he argued.