Weekly Intelligence Summary

Dec 11, 2020 (TLP: WHITE)

In the spotlight this week:

- Microsoft patched a SMB remote information disclosure vulnerability this patch tuesday I reported in September, it may affect over Windows 7 to Windows 10, more detail you can find in MSRC. I will public the vulnerability detail in this blog. The root cause of CVE-2020-17140 is a code logic error that will cause use after free, vulnerability exists in srv2!Smb2UpdateLeaseFileName, k0shl of Vulcan Team said.
  #CVSS:3.0 8.1/7.1 <- what does it mean? #Unimportant?
- Today, we're sharing actions we took against two separate groups of hackers — APT32 in Vietnam and a group based in Bangladesh. Our investigation linked this activity to two non-profit organizations in Bangladesh: Don's Team and the Crime Research and Analysis Foundation . They appeared to be operating across a number of internet services. APT32, an advanced persistent threat actor based in Vietnam, targeted Vietnamese human rights activists locally and abroad, various foreign governments including those in Laos and Cambodia, non-governmental organizations, news agencies and a number of businesses. Our investigation linked this activity to CyberOne Group, an IT company in Vietnam. Facebook said.
- On December 11th, Able Soft stated in an email to us that the trojanized installers and Able Desktop's updates have not been used since the incident was reported to them. They also stated that, as a precaution against further attacks, Able Soft halted the Able Desktop updates, and that the last occurrence they observed of such attacks was in July 2020, ESET said. #SupplyChainAttack #NotSolarWind
- A highly sophisticated state-sponsored adversary stole FireEye Red Team tools. Because we believe that an adversary possesses these tools, and we do not know whether the attacker intends to use the stolen tools themselves or publicly disclose them, FireEye is releasing hundreds of countermeasures with this blog post to enable the broader security community to protect themselves against these tools. We have incorporated the countermeasures in our FireEye products—and shared these countermeasures with partners, government agencies—to significantly limit the ability of the bad actor to exploit the Red Team tools. They also share a list of countermeasures on the FireEye Github. I appreciate their responsible attitude to disclose their breach. #VPN, #NoProveLinkToSolarWind

(cisp-id:9731) Dec 11, 2020
CVE-2020-17140 Windows SMB Information Disclosure Analysis.
Microsoft patched a SMB remote information disclosure vulnerability this patch tuesday I reported in September, it may affect over Windows 7 to Windows 10, more detail you can find in MSRC Acknowledgements: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17140 , I will public the vulnerability detail in this blog. The root cause of CVE-2020-17140 is a code logic error that will cause use after free, vulnerability exists in srv2!Smb2UpdateLeaseFileName, k0shl of Vulcan Team said. #CVSS:3.0 8.1/7.1 <- what does it mean? #Unimportant?
https://blogs.360.cn/post/CVE-2020-17140-Analysis.html

(cisp-id:9695) Dec 10, 2020
Taking Action Against Hackers in Bangladesh and Vietnam.
Today, we're sharing actions we took against two separate groups of hackers — APT32 in Vietnam and a group based in Bangladesh — removing their ability to use their infrastructure to abuse our

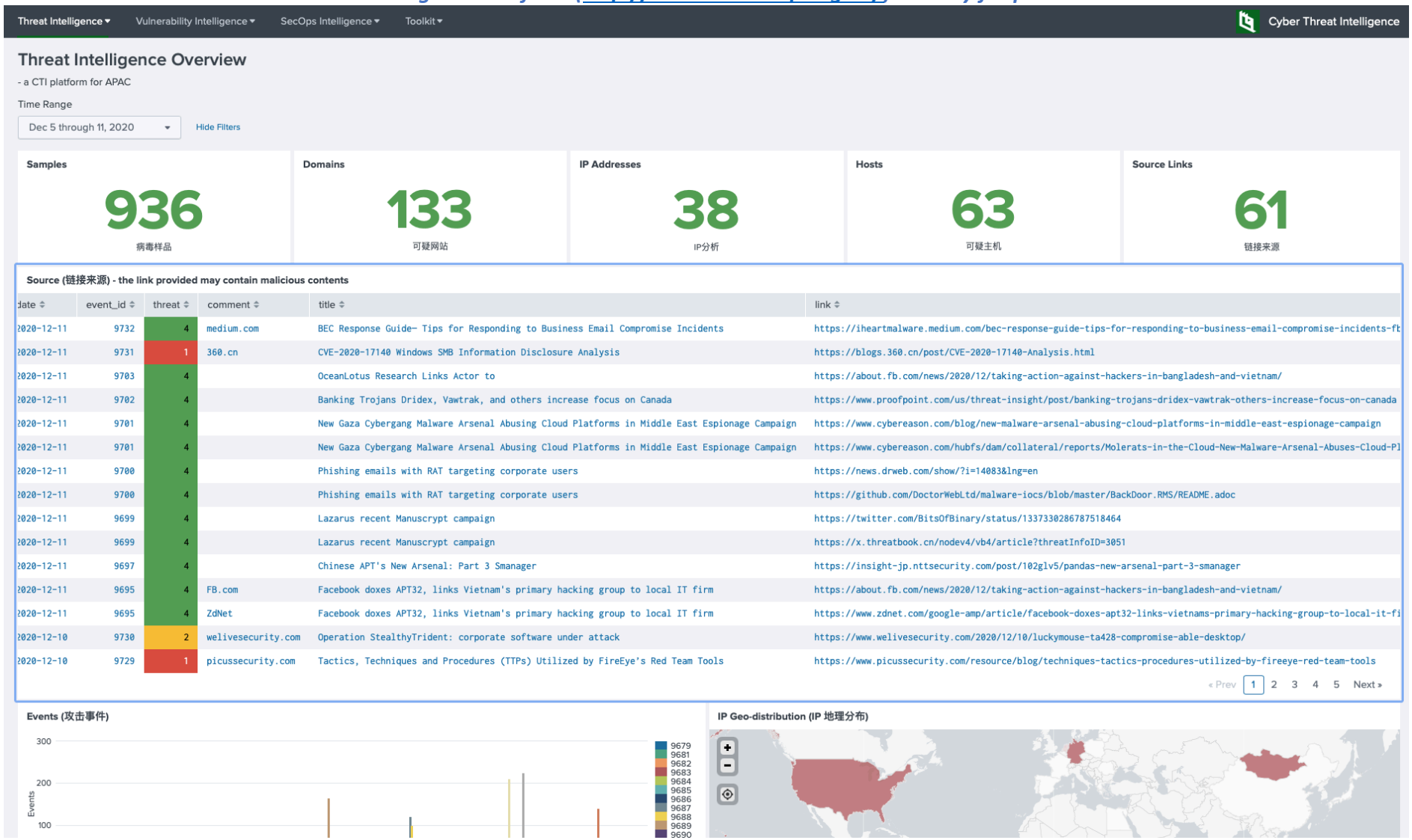
platform, distribute malware and hack people's accounts across the internet. Our investigation linked this activity to two non-profit organizations in Bangladesh: Don's Team (also known as Defense of Nation) and the Crime Research and Analysis Foundation (CRAF). They appeared to be operating across a number of internet services. APT32, an advanced persistent threat actor based in Vietnam, targeted Vietnamese human rights activists locally and abroad, various foreign governments including those in Laos and Cambodia, non-governmental organizations, news agencies and a number of businesses across information technology, hospitality, agriculture and commodities, hospitals, retail, the auto industry, and mobile services with malware. Our investigation linked this activity to CyberOne Group, an IT company in Vietnam.
https://about.fb.com/news/2020/12/taking-action-against-hackers-in-bangladesh-and-vietnam/

(cisp-id:9730) Dec 10, 2020
Operation StealthyTrident: LuckyMouse, TA428, HyperBro, Tmanger and ShadowPad linked in Mongolian supply-chain attack.
On December 11th, Able Soft stated in an email to us that the trojanized installers and Able Desktop's updates have not been used since the incident was reported to them. They also stated that, as a precaution against further attacks, Able Soft halted the Able Desktop updates, and that the last occurrence they observed of such attacks was in July 2020. ESET researchers discovered that chat software called Able Desktop, part of a business management suite popular in Mongolia and used by 430 government agencies in Mongolia (according to Able), was used to deliver the HyperBro backdoor (commonly used by LuckyMouse), the Korplug RAT (also known as PlugX), and a RAT called Tmanger (which was first documented by NTT Security and was used during Operation Lagtime IT campaigns attributed to TA428 by Proofpoint). A connection with the ShadowPad backdoor, which is now used by at least five different threat actors, was also found.
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/

(cisp-id:9722) Dec 9, 2020
Paloalto Unit 42: VMware Command Injection Vulnerability (CVE-2020-4006).
On Dec. 7, 2020, the National Security Agency (NSA) published a cybersecurity advisory indicating they observed Russian state-sponsored actors exploiting a VMware command injection vulnerability (CVE-2020-4006). VMware issued a patch for the vulnerability on Dec. 3, 2020. Password-based access to the web-based management interface of the device is required to exploit the vulnerability, so using a strong and unique password lowers the risk of exploitation. The risk is lowered further if the web-based management interface is not accessible from Internet. NSA said in a Cybersecurity Alert.
https://unit42.paloaltonetworks.com/cve-2020-4006/
https://media.defense.gov/2020/Dec/07/2002547071/-1/-1/0/CSA_VMWARE%20ACCESS_U_OO_195076_20.PDF

(cisp-id:9735) Dec 8, 2020
FireEye: Unauthorized Access of FireEye Red Team Tools.
A highly sophisticated state-sponsored adversary stole FireEye Red Team tools. Because we believe that an adversary possesses these tools, and we do not know whether the attacker intends to use the stolen tools themselves or publicly disclose them, FireEye is releasing hundreds of countermeasures with this blog post to enable the broader security community to protect themselves against these tools. We have incorporated the countermeasures in our FireEye products—and shared these countermeasures with partners, government agencies—to significantly limit the ability of the bad actor to exploit the Red Team tools.
https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html
https://www.picussecurity.com/resource/blog/techniques-tactics-procedures-utilized-by-fireeye-red-team-tools

Our Threat Intelligence Platform (http://dashboard.cisp.org.hk/) is ready for public access.



Get access? please send an email to: admin@dragonadvancetech.com