Weekly Intelligence Summary

Nov 20, 2020 (TLP: WHITE)

In the spotlight this week:

- Cloudflare observed some key network layer DDoS trends in Q3: (1) Majority of the attacks are under 500 Mbps and 1 Mpps — both still suffice to cause service disruptions, (2) Continue to see a majority of attacks be under 1 hr in duration, and (3) Ransom-driven DDoS attacks (***RDDoS***) are on the rise as groups ***claiming to be Fancy Bear, Cozy Bear and the Lazarus Group*** extort organizations around the world.
- Cisco plans to fix ***three vulnerabilities in the Webex*** video conferencing app that can allow attackers to sneak in and join Webex meetings as ghost users, invisible to other participants. Researchers said the three bugs, when combined, would have allowed an attacker to: (1) Join a Webex meeting as a ***ghost user***, (2) Remain in a Webex meeting as a ghost and (3) Obtain information on meeting participants.
- Unit 42 researchers discovered a class of Amazon Web Services (AWS) APIs that can be abused to ***leak the AWS IAM users and roles*** in arbitrary accounts. Researchers confirmed that 22 APIs across 16 different AWS services could be abused the same way and the exploit works across all three AWS partitions (aws, aws-us-gov or aws-cn). AWS services that can be potentially abused by attackers include Amazon Simple Storage Service (S3), Amazon Key Management Service (KMS) and Amazon Simple Queue Service (SQS). The root cause of the issue is that the AWS backend proactively validates all the resource-based policies attached to resources such as Amazon Simple Storage Service (S3) buckets and customer-managed keys.
- Cisco has patched ***two vulnerabilities*** in its ***Cisco Security Manager solution***, both of which could allow unauthenticated, remote attackers to gain access to sensitive information on an affected system. Those are part of a batch of twelve vulnerabilities flagged in July 2020 by Florian Hauser, a security researcher and red teamer at Code White. Hauser ***shared PoCs*** for the flaws he discovered and flagged.
- A large-scale attack campaign is ***targeting multiple Japanese companies***, including subsidiaries located in as many as 17 regions around the globe. Companies in multiple sectors are targeted in this campaign, including those operating in the automotive, pharmaceutical, and engineering sector, as well as MSPs. Symantec is discovering enough evidence to ***attribute it to Cicada*** (aka APT10, Stone Panda, Cloud Hopper). The attackers also use DLL side-loading at multiple stages during the attack, including using it to load Backdoor.Hartip. a dropped DLL has an export named "FuckYouAnti".

(cisp-id:9567) Nov 20, 2020
VMware Patches Vulnerabilities Exploited at Chinese Hacking Contest.
The 360 ESG Vulnerability Research Institute from Chinese cybersecurity company Qihoo 360 earned more than $740,000 of the total, including $180,000 for a VMware ESXi guest to host escape exploit. VMware was monitoring the event and it immediately started working on patches. The virtualization giant announced the first patches on Thursday, less than two weeks after Tianfu Cup ended. One of the security holes, CVE-2020-4005, is a privilege escalation issue caused by the way certain system calls are managed. This high-severity flaw allows an attacker who has privileges within the VMX process only to elevate permissions on the targeted system.
https://www.securityweek.com/vmware-patches-vulnerabilities-exploited-chinese-hacking-contest

(cisp-id:9567) Nov 18, 2020
Network-layer DDoS attack trends for Q3 2020.
Cloudflare observed some key network layer DDoS trends in Q3:

(1) Majority of the attacks are under 500 Mbps and 1 Mpps — both still suffice to cause service disruptions, (2) Continue to see a majority of attacks be under 1 hr in duration, and (3) Ransom-driven DDoS attacks (RDDoS) are on the rise as groups claiming to be Fancy Bear, Cozy Bear and the Lazarus Group extort organizations around the world.
https://www.cloudflare.com/learning/ddos/ransom-ddos-attack/

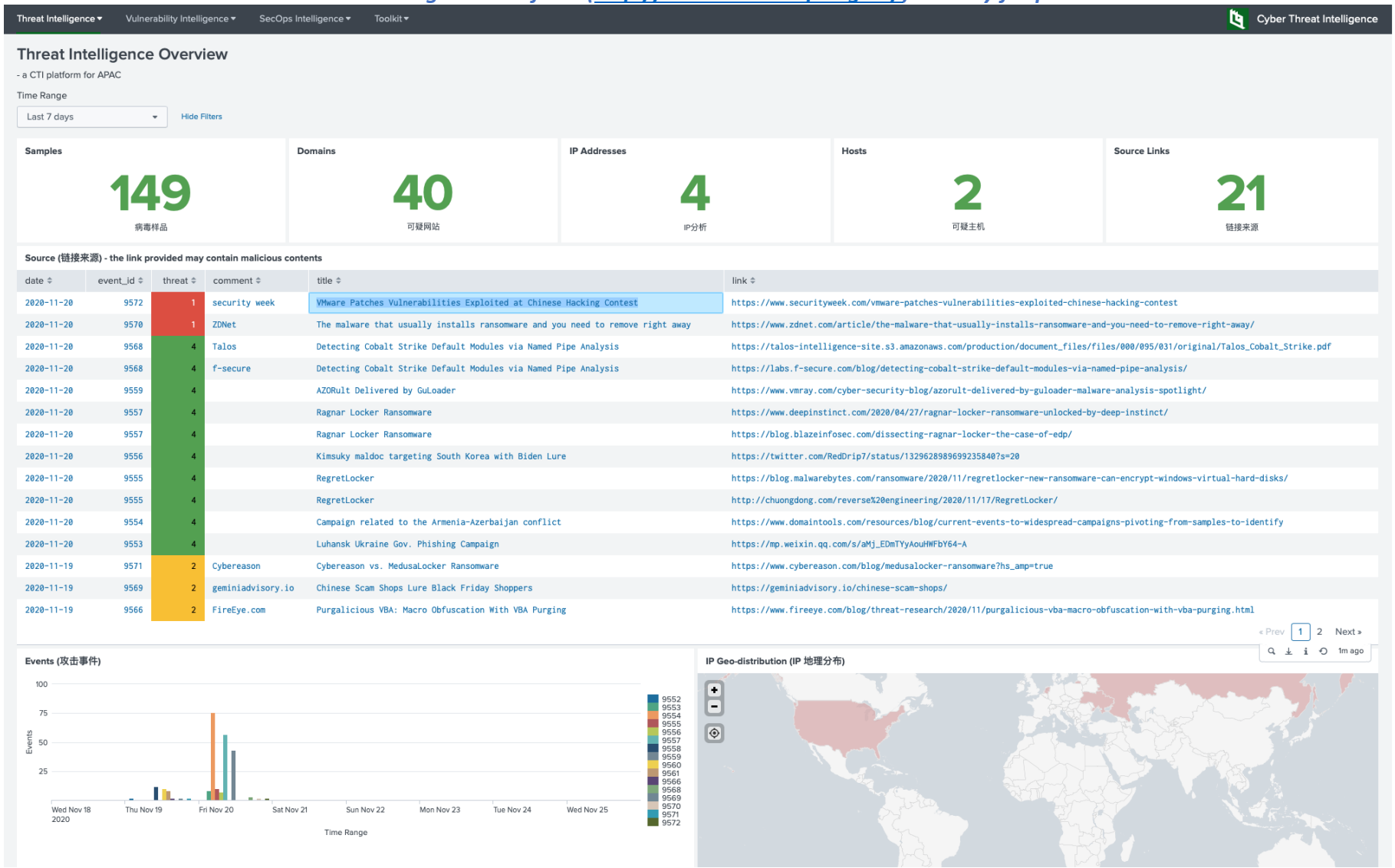
(cisp-id:9551) Nov 18, 2020
Cisco Webex bugs allow attackers to join meetings as ghost users.
Cisco plans to fix three vulnerabilities in the Webex video conferencing app that can allow attackers to sneak in and join Webex meetings as ghost users, invisible to other participants. The vulnerabilities were discovered earlier this year by security researchers from IBM, who conducted a review of remote working tools the tech software giant was using internally during the coronavirus pandemic. Researchers said the three bugs, when combined, would have allowed an attacker to: (1) Join a Webex meeting as a ghost user, (2) Remain in a Webex meeting as a ghost and (3) Obtain information on meeting participants.
https://www.zdnet.com/article/cisco-webex-bugs-allow-attackers-to-join-meetings-as-ghost-users/#ftag=RSSbaffb68

(cisp-id:9540) Nov 17, 2020
Information Leakage in AWS Resource-Based Policy APIs.
Unit 42 researchers discovered a class of Amazon Web Services (AWS) APIs that can be abused to leak the AWS Identity and Access Management (IAM) users and roles in arbitrary accounts. Researchers confirmed that 22 APIs across 16 different AWS services could be abused the same way and the exploit works across all three AWS partitions (aws, aws-us-gov or aws-cn). AWS services that can be potentially abused by attackers include Amazon Simple Storage Service (S3), Amazon Key Management Service (KMS) and Amazon Simple Queue Service (SQS). The root cause of the issue is that the AWS backend proactively validates all the resource-based policies attached to resources such as Amazon Simple Storage Service (S3) buckets and customer-managed keys.
https://unit42.paloaltonetworks.com/aws-resource-based-policy-apis/

(cisp-id:9531) Nov 17, 2020
Japan-Linked Organizations Targeted in Long-Running and Sophisticated Attack Campaign.
A large-scale attack campaign is targeting multiple Japanese companies, including subsidiaries located in as many as 17 regions around the globe in a likely intelligence-gathering operation. Companies in multiple sectors are targeted in this campaign, including those operating in the automotive, pharmaceutical, and engineering sector, as well as managed service providers (MSPs). The scale and sophistication of this attack campaign indicates that it is the work of a large and well-resourced group, with Symantec, discovering enough evidence to attribute it to Cicada (aka APT10, Stone Panda, Cloud Hopper).The companies hit are, in the main, large, well-known organizations, many of which have links to Japan or Japanese companie. The attackers also use DLL side-loading at multiple stages during the attack, including using it to load Backdoor.Hartip. The DLL has an export named "FuckYouAnti".
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage

(cisp-id:9522) Nov 12, 2020
“Email Appender” Implants Malicious Emails Directly Into Mailboxes
ESET researchers have discovered a sophisticated backdoor that allows attackers to access sensitive data stored in systems used in the hospitality sector, such as the RES 3700 POS management software, which is used by hundreds of thousands of hotels and restaurants worldwide. What makes the backdoor distinctive are its downloadable modules and their capabilities.
https://www.cyberscoop.com/email-appender-implant-gemini-advisory/

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



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