Weekly Intelligence Summary

Nov 13, 2020 (TLP: WHITE)

In the spotlight this week:

- ***Ubuntu*** fixes bugs that standard users could use to become root. The first series of commands triggered a denial-of-service bug in a daemon called ***accountsservice***, which as its name suggests is used to manage user accounts on the computer. To do this, Backhouse created a Symlink, changed the regional language setting, and sent accountsservice a SIGSTOP. With the help of a few extra commands, Backhouse was able to set a timer that gave him just enough time to log out of the account before accountsservice crashed. When done correctly, Ubuntu would restart and open a window that allowed the user to ***create a new account*** that—you guessed it—had ***root privileges***.
- ***Adobe and Microsoft*** each issued a bevy of updates today to plug critical security holes in their software. Microsoft’s release includes fixes for 112 separate flaws, including one zero-day vulnerability that is already being exploited to attack Windows users. ***A chief concern*** among all these updates this month is CVE-2020-17087, which is an “important” bug in the Windows kernel that is already seeing active exploitation. ***CVE-2020-17087 is not listed as critical*** because it’s what’s known as a privilege escalation flaw that would allow an attacker who has already compromised a less powerful user account on a system to gain administrative control. In essence, it would have to ***be chained with another exploit***.
- PaloAlto observed involved two backdoors – one of which we call ***TriFive*** and a variant of CASHY200 that we call ***Snugy*** – as well as a web shell that we call ***BumbleBee***. The TriFive and Snugy backdoors are PowerShell scripts that provide backdoor access to the compromised Exchange server, using ***Exchange Web Services (EWS)*** to create drafts within the Deleted Items folder of a compromised email account. The Snugy backdoor uses a ***DNS tunneling*** channel to run commands on the compromised server.
- Sophos said: A group of targeted attacks takes a different spin on methods first seen in ***PlugX APT***. The cases are connected by a common artifact: the program database (PDB) path. All samples share a similar PDB path, with several of them containing the folder name “***KillSomeOne***.” They have identified four different ***side-loading scenarios*** (a clean loader calling a malicious dll to decrypt play load with a file of .dat) that were used by the same threat actor. I remembered I had analysed various sample sets using similar TTP in a ***intrusion analysis*** for a ***Hong Kong*** university in 2017. I even used asked my students to create a yara rule in an examination question. ;)
- Mandiant has been investigating ***compromised Oracle Solaris*** machines in customer environments. During our investigations, we discovered an exploit tool on a customer’s system and analyzed it to see how it was attacking their Solaris environment. Mandiant experts provided detailed information on this vulnerability and how it was used by ***UNC1945*** during a webinar. They also developed a ***proof of concept*** exploit to trigger the overflow and crash the SSH server.

(cisp-id:9508) Nov 11, 2020

Ubuntu fixes bugs that standard users could use to become root.

The first series of commands triggered a denial-of-service bug in a daemon called accountsservice, which as its name suggests is used to manage user accounts on the computer. To do this, Backhouse created a Symlink, changed the regional language setting, and sent accountsservice a SIGSTOP. With the help of a few extra commands, Backhouse was able to set a timer that gave him just enough time to log out of the account before accountsservice crashed. When done correctly, Ubuntu would

restart and open a window that allowed the user to create a new account that—you guessed it—had root privileges. Here's a video of Backhouse's attack in action.
https://arstechnica.com/information-technology/2020/11/ubuntu-fixes-bugs-that-standard-users-could-use-to-become-root/

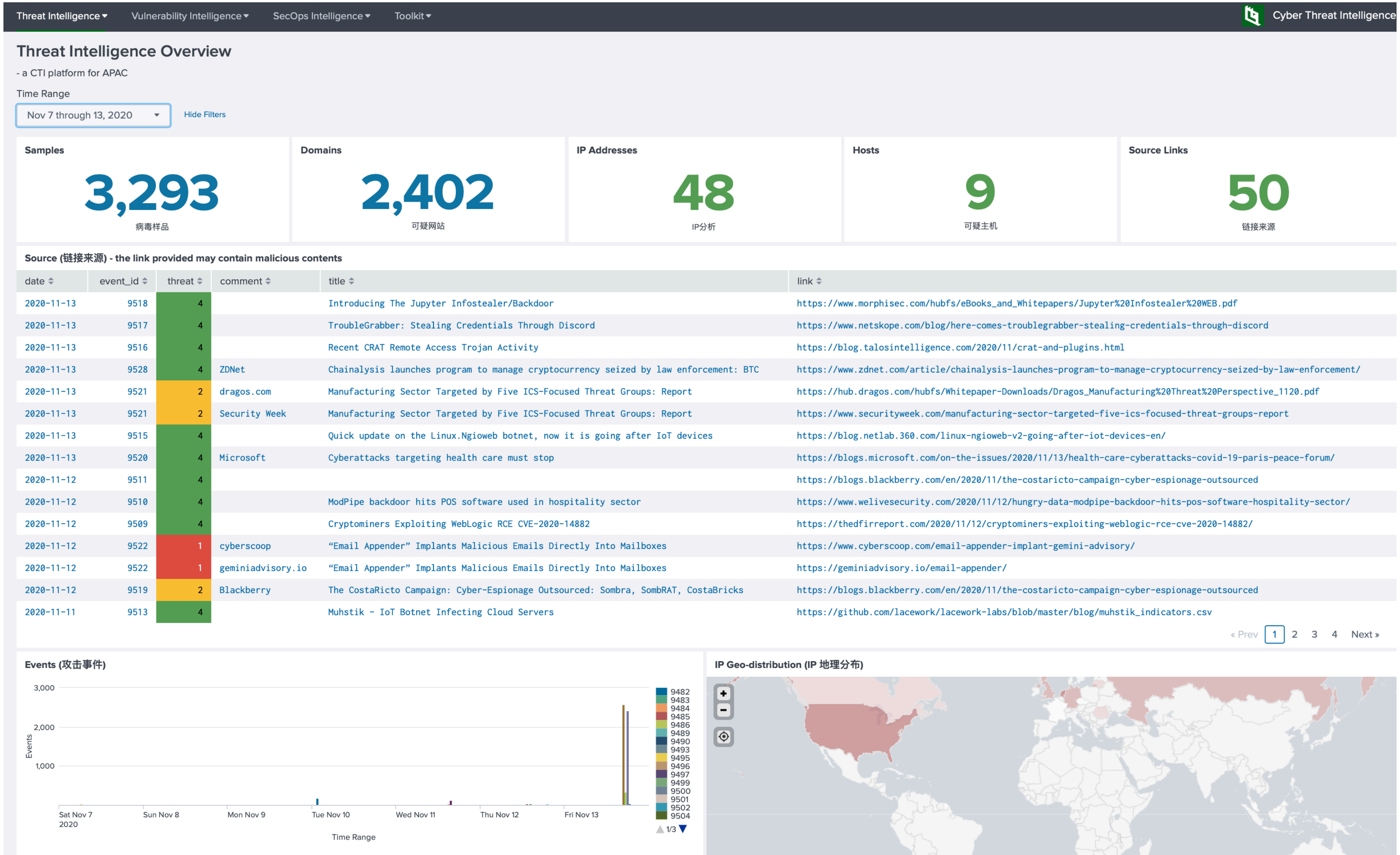
(cisp-id:9506) Nov 10, 2020
Adobe's Security Updates for Multiple Products and Microsfot Patch Tuesday, Nov Edition
Adobe and Microsoft each issued a bevy of updates today to plug critical security holes in their software. Microsoft's release includes fixes for 112 separate flaws, including one zero-day vulnerability that is already being exploited to attack Windows users. Microsoft also is taking flak for changing its security advisories and limiting the amount of information disclosed about each bug. A chief concern among all these updates this month is CVE-2020-17087, which is an "important" bug in the Windows kernel that is already seeing active exploitation. CVE-2020-17087 is not listed as critical because it's what's known as a privilege escalation flaw that would allow an attacker who has already compromised a less powerful user account on a system to gain administrative control. In essence, it would have to be chained with another exploit.
https://krebsonsecurity.com/2020/11/patch-tuesday-november-2020-edition/

(cisp-id:9502) Nov 9, 2020
Newly Backdoors Using Deleted Email Drafts and DNS Tunneling for Command and Control.
The xHunt campaign has been active since at least July 2018 and we have seen this group target Kuwait government and shipping and transportation organizations. The activity PaloAlto observed involved two backdoors – one of which we call TriFive and a variant of CASHY200 that we call Snugy – as well as a web shell that we call BumbleBee. The TriFive and Snugy backdoors are PowerShell scripts that provide backdoor access to the compromised Exchange server, using Exchange Web Services (EWS) to create drafts within the Deleted Items folder of a compromised email account. The Snugy backdoor uses a DNS tunneling channel to run commands on the compromised server.
https://unit42.paloaltonetworks.com/xhunt-campaign-backdoors/

(cisp-id:9493) Nov 7, 2020
A new APT uses DLL side-loads to "KilllSomeOne"
Sophos said: A group of targeted attacks takes a different spin on methods first seen in PlugX APT operations. They first saw it used by (mostly Chinese) APT groups as early as 2013, before cybercrime groups started to add it to their arsenal—this particular payload was not one we've seen before. It stands out because the threat actors used several plaintext strings written in poor English with politically inspired messages in their samples. The cases are connected by a common artifact: the program database (PDB) path. All samples share a similar PDB path, with several of them containing the folder name "KilllSomeOne." They have identified four different side-loading scenarios (a clean loder calling a malicious dll to decrypt a playload with extension .dat) that were used by the same threat actor.
https://news.sophos.com/en-us/2020/11/04/a-new-apt-uses-dll-side-loads-to-killlsomeone/

(cisp-id:9490) Nov 7, 2020
In Wild Critical Buffer Overflow Vulnerability in Solaris— CVE-2020-14871.
Mandiant has been investigating compromised Oracle Solaris machines in customer environments. During our investigations, we discovered an exploit tool on a customer's system and analyzed it to see how it was attacking their Solaris environment. Mandiant experts provided detailed information on this vulnerability and how it was used by UNC1945 during a webinar. They also developed a proof of concept exploit to trigger the overflow and crash the SSH server.
https://www.fireeye.com/blog/threat-research/2020/11/critical-buffer-overflow-vulnerability-in-solaris-can-allow-remote-takeover.html

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



Threat Intelligence Overview

- a CTI platform for APAC

Time Range: Nov 7 through 13, 2020

Samples	Domains	IP Addresses	Hosts	Source Links
3,293	2,402	48	9	50
病毒样品	可疑网站	IP分析	可疑主机	链接来源

Source (链接来源) - the link provided may contain malicious contents

date	event_id	threat	comment	title	link
2020-11-13	9518	4		Introducing The Jupyter Infostealer/Backdoor	https://www.morphisec.com/hubfs/eBooks_and_Whitepapers/Jupyter%20Infostealer%20WEB.pdf
2020-11-13	9517	4		TroubleGrabber: Stealing Credentials Through Discord	https://www.netskope.com/blog/here-comes-troublegrabber-stealing-credentials-through-discord
2020-11-13	9516	4		Recent CRAT Remote Access Trojan Activity	https://blog.talosintelligence.com/2020/11/crat-and-plugins.html
2020-11-13	9528	4	ZDNet	Chainalysis launches program to manage cryptocurrency seized by law enforcement: BTC	https://www.zdnet.com/article/chainalysis-launches-program-to-manage-cryptocurrency-seized-by-law-enforcement/
2020-11-13	9521	2	dragos.com	Manufacturing Sector Targeted by Five ICS-Focused Threat Groups: Report	https://hub.dragos.com/hubfs/Whitepaper-Downloads/Dragos_Manufacturing%20Threat%20Perspective_1120.pdf
2020-11-13	9521	2	Security Week	Manufacturing Sector Targeted by Five ICS-Focused Threat Groups: Report	https://www.securityweek.com/manufacturing-sector-targeted-five-ics-focused-threat-groups-report
2020-11-13	9515	4		Quick update on the Linux.Ngioweb botnet, now it is going after IoT devices	https://blog.netlab.360.com/linux-ngioweb-v2-going-after-iot-devices-en/
2020-11-13	9520	4	Microsoft	Cyberattacks targeting health care must stop	https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/
2020-11-12	9511	4			https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced
2020-11-12	9510	4		ModPipe backdoor hits POS software used in hospitality sector	https://www.welivesecurity.com/2020/11/12/hungry-data-modpipe-backdoor-hits-pos-software-hospitality-sector/
2020-11-12	9509	4		Cryptominers Exploiting WebLogic RCE CVE-2020-14882	https://thedfirreport.com/2020/11/12/cryptominers-exploiting-weblogic-rce-cve-2020-14882/
2020-11-12	9522	1	cyberscoop	“Email Appender” Implants Malicious Emails Directly Into Mailboxes	https://www.cyberscoop.com/email-appender-implant-gemini-advisory/
2020-11-12	9522	1	geminiadvisory.io	“Email Appender” Implants Malicious Emails Directly Into Mailboxes	https://geminiadvisory.io/email-appender/
2020-11-12	9519	2	Blackberry	The CostaRicto Campaign: Cyber-Espionage Outsourced: Sombra, SombRAT, CostaBricks	https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced
2020-11-11	9513	4		Muhstik - IoT Botnet Infecting Cloud Servers	https://github.com/lacework/lacework-labs/blob/master/blog/muhstik_indicators.csv

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