Dragon Advance Tech

Weekly Intelligence Summary

Nov 27, 2020 (TLP: WHITE)

In the spotlight this week:

- A complex phishing scheme has been active for more than half a year for stealing Office 365 credentials from SME in the U.S. and Australia combines cloud services from Amazon Web Services and Oracle Cloud into its infrastructure. The campaign and uses a network of legitimate websites that have been compromised to work as a proxy chain. The operators bait recipients with fake notifications for voice messages and Zoom invitations that ultimately lead the victim to the phishing page collecting login credentials. Cybersecurity company Mitiga says that despite the simple lure and purpose, the campaign stands out as sophisticated as the road to exfiltration goes through legitimate services and websites.
- Check Point Research recently observed a new wave of campaigns against various targets worldwide that utilizes a strain of a 13-year old backdoor Trojan named Bandook. During 2015-17, dozens of digitally signed variants of this once commodity malware started to reappear in the threat landscape, reigniting interest in this old malware family. The full infection chain of the attack can be broken down into three main stages: (1) Lure document that loads external template with malicious VBA code, (2) PowerShell loader downloads encoed executable parts from Dropbox and constructs the Bandookr loader executable, and (3) Bankdoor loader utilizes process hollowing to inject the Bandook backdoor into a new Internet explorer process.
- An exploitation of critical FortiOS vulnerability CVE-2018-13379 lets an attacker access the sensitive "sslvpn_websession" files from Fortinet VPNs. These files contain session-related information, may reveal plain text usernames and passwords of Fortinet VPN users. Threat intelligence analyst Bank_Security has found another thread on the hacker forum where a threat actor shared a data dump containing "sslvpn_websession" files for every IP that had been on the list. As observed by BleepingComputer, these files reveal usernames, passwords, access levels (e.g. "full-access"), and the original unmasked IP addresses of users connected to the VPNs. After a nslookup on all IPs, I found that among the victims there are some Banks, many .gov domains and thousands of companies around the world, @Bank_Security said. We found the leaked files shows IPs around US, India and Japan and 927 records from #HongKong.

(cisp-id:9640) Nov 27, 2020

Office 365 phishing abuses Oracle and Amazon cloud services.

A rather complex phishing scheme for stealing Office 365 credentials from small and medium-sized businesses in the U.S. and Australia combines cloud services from Oracle and Amazon into its infrastructure. The campaign has been active for more than half a year and uses a network of legitimate websites that have been compromised to work as a proxy chain. The operators bait recipients with fake notifications for voice messages and Zoom invitations that ultimately lead the victim to the phishing page collecting login credentials. Cybersecurity company Mitiga says that despite the simple lure and purpose, the campaign stands out as sophisticated as the road to exfiltration goes through legitimate services and websites. According to their research, the threat actor sends phishing messages from compromised email accounts and uses Amazon Web Services (AWS) and Oracle Cloud in the redirect chain.

https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/office-365-phishing-abuses-oracle-and-amazon-cloud-services/amp/

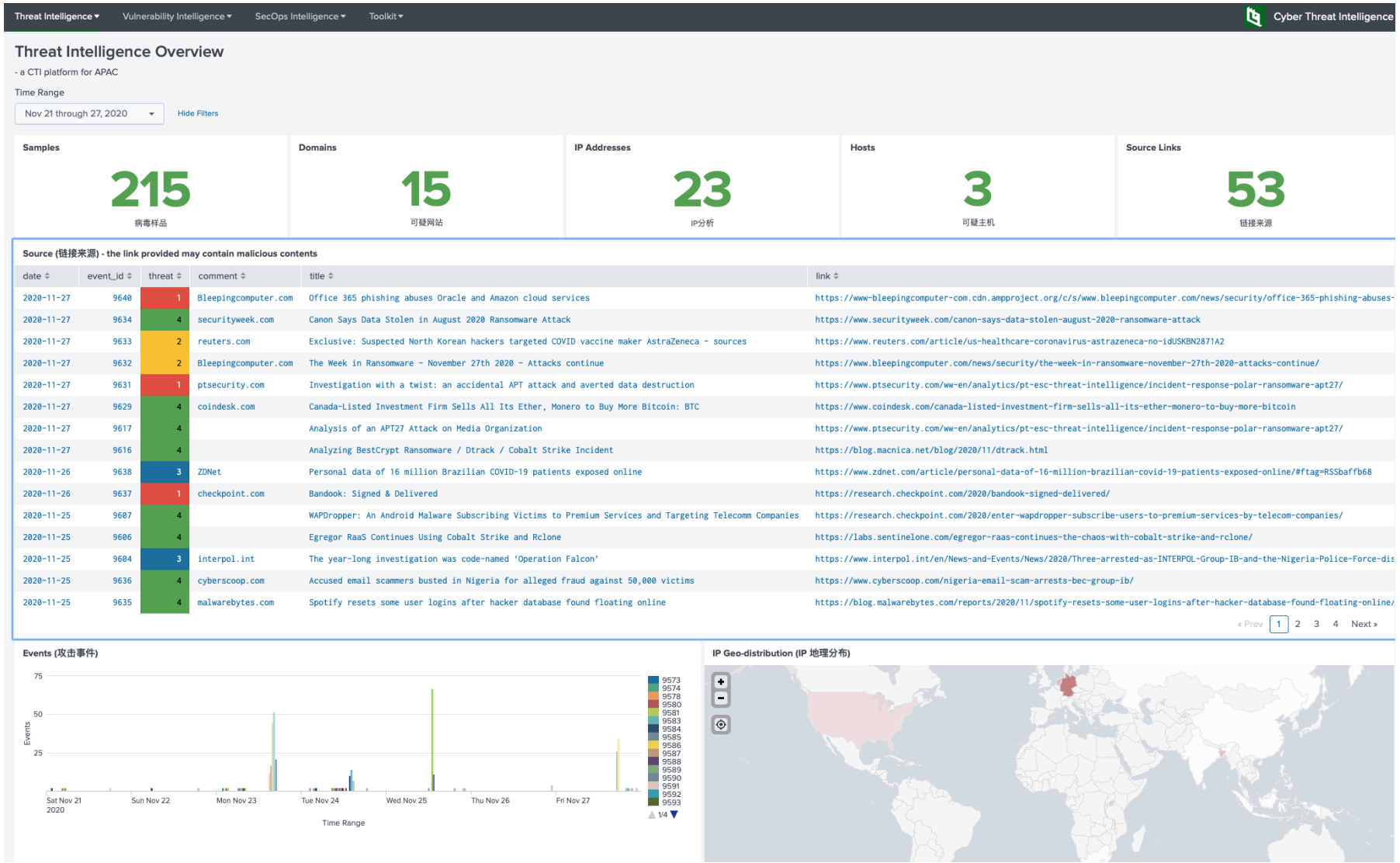
(cisp-id:9637) Nov 26, 2020
Bandook: Signed & Delivered.
Check Point Research recently observed a new wave of campaigns against various targets worldwide that utilizes a strain of a 13-year old backdoor Trojan named Bandook. In 2015 and 2017 these campaigns were presumed to be carried out by the Kazakh and the Lebanese governments. During this past year, dozens of digitally signed variants of this once commodity malware started to reappear in the threat landscape, reigniting interest in this old malware family. In the latest wave of attacks, we once again identified an unusually large variety of targeted sectors and locations. The full infection chain of the attack can be broken down into three main stages: (1) Lure document that loads external template with malicious VBA code, (2) PowerShell loader downloads encoed executable parts from Dropbox and constructs the Bandookr loader executable, and (3) Bankdoor loader utilizes process hollowing to inject the Bandook backdoor into a new Internet explorer process.
https://research.checkpoint.com/2020/bandook-signed-delivered/

(cisp-id:9604) Nov 25, 2020
Three arrested as INTERPOL, Group-IB and the Nigeria Police Force disrupt prolific cybercrime group.
Three suspects have been arrested in Lagos following a joint INTERPOL, Group-IB and Nigeria Police Force cybercrime investigation. The suspects are alleged to have developed phishing links, domains, and mass mailing campaigns in which they impersonated representatives of organizations. They then used these campaigns to disseminate 26 malware programmes, spyware and remote access tools, including AgentTesla, Loki, Azorult, Spartan and the nanocore and Remcos Remote Access Trojans. These programmes were used to infiltrate and monitor the systems of victim organizations and individuals, before launching scams and syphoning funds. According to Group-IB, the prolific gang is believed to have compromised government and private sector companies in more than 150 countries since 2017.
https://www.interpol.int/en/News-and-Events/News/2020/Three-arrested-as-INTERPOL-Group-IB-and-the-Nigeria-Police-Force-disrupt-prolific-cybercrime-group

(cisp-id:9635) Nov 25, 2020
Spotify resets some user logins after hacker database found floating online.
A team of researchers working for vpnMentor has found a treasure trove in the form of an unsecured Elasticsearch database containing over 380 million records. The trove contained login credentials and other data belonging to Spotify users. The origins of the database and how the fraudsters were targeting Spotify are both unknown. After port scanning and examining weaknesses and vulnerabilities, the researchers habitually look for leaked data. This database was unsecured and unencrypted, so it was fully accessible for anyone that found it. The hackers were possibly using login credentials stolen from another platform, app, or website and using them to access Spotify accounts, vpnMentor said.
https://blog.malwarebytes.com/reports/2020/11/spotify-resets-some-user-logins-after-hacker-database-found-floating-online/

(cisp-id:9626) Nov 25, 2020
Passwords exposed for almost 50,000 vulnerable Fortinet VPNs.
The exploitation of critical FortiOS vulnerability CVE-2018-13379 lets an attacker access the sensitive "sslvpn_websession" files from Fortinet VPNs. These files contain session-related information, but most importantly, may reveal plain text usernames and passwords of Fortinet VPN users. Today, threat intelligence analyst Bank_Security has found another thread on the hacker forum where a threat actor shared a data dump containing "sslvpn_websession" files for every IP that had been on the list. As observed by BleepingComputer, these files reveal usernames, passwords, access levels (e.g. "full-access"), and the original unmasked IP addresses of users connected to the VPNs.
https://www.bleepingcomputer.com/news/security/passwords-exposed-for-almost-50-000-vulnerable-fortinet-vpns/

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



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