Dragon Advance Tech

Weekly Intelligence Summary

Sep 25, 2020 (TLP: WHITE)

In the spotlight this week:

- A hacker has gained access and ***exfiltrated data from a federal agency***, the Cybersecurity and Infrastructure Security Agency (CISA) said. The cyber threat actor had valid access credentials for multiple users' ***Microsoft Office 365 (O365) accounts*** and domain administrator accounts, which they leveraged for Initial Access to the agency's network. In April 2019, Pulse Secure released patches for several critical vulnerabilities—including ***CVE-2019-11510***, which allows the remote, unauthenticated retrieval of files, including passwords. CISA has observed wide exploitation of ***CVE-2019-11510*** across the federal government. ***#O365-compromise-with-data-breach***
- ***Shopify*** discloses security incident caused by two rogue employees. The online e-commerce giant Shopify is working with the FBI and other law enforcement agencies to investigate ***a security breach*** caused by two ***rogue employees***. The company said two members of its support team accessed and tried to obtain customer transaction details from Shopify shop owners (merchants).
- Paloalto has seen significantly more Emotet malspam using a technique called "***thread hijacking***" that utilizes legitimate messages stolen from infected computers' email clients. This malspam spoofs a legitimate user and impersonates a reply to the stolen email. Thread hijacked malspam is sent to addresses from the original message. This technique is much more effective than less sophisticated methods, which many people have now learned to spot. ***#TargetPhishing***
- Medical labs, banks, manufacturers and software developers in Russia are the prime targets for a new ransomware gang that began operating with custom tools as early as March of this year, according to researchers at the security vendor Group-IB. The attackers insert their hacking tools into networks via malware downloaded through ***spearphishing emails***, then encrypt files and hold them ransom for about $50,000, Group IB says. The group, dubbed OldGremlin, has only targeted Russian companies so far, Group-IB says. It's rare for a Russian-speaking ransomware group to aim at targets inside Russia.

(cisp-id:9234) Sep 24, 2020

CISA says a hacker breached a federal agency.

A hacker has gained access and exfiltrated data from a federal agency, the Cybersecurity and Infrastructure Security Agency (CISA) said on Thursday. The cyber threat actor had valid access credentials for multiple users' Microsoft Office 365 (O365) accounts and domain administrator accounts, which they leveraged for Initial Access to the agency's network. First the threat actor logged into a user's O365 account from Internet Protocol (IP) address 91.219.236[.]166 and then browsed pages on a SharePoint site and downloaded a file. The cyber threat actor connected multiple times from IP address 185.86.151[.]223 to the victim organization's virtual private network (VPN) server. CISA analysts were not able to determine how the cyber threat actor initially obtained the credentials. In April 2019, Pulse Secure released patches for several critical vulnerabilities—including CVE-2019-11510, which allows the remote, unauthenticated retrieval of files, including passwords.CISA has observed wide exploitation of CVE-2019-11510 across the federal government.
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-268a

(cisp-id:9229) Sep 23, 2020
Shopify discloses security incident caused by two rogue employees.
Online e-commerce giant Shopify is working with the FBI and other law enforcement agencies to investigate a security breach caused by two rogue employees. The company said two members of its support team accessed and tried to obtain customer transaction details from Shopify shop owners (merchants). The e-commerce giant said the incident is not the result of a vulnerability in its platform but the actions of rogue employees.
https://www.zdnet.com/article/shopify-discloses-security-incident-caused-by-two-rogue-employees/#ftag=RSSbaffb68

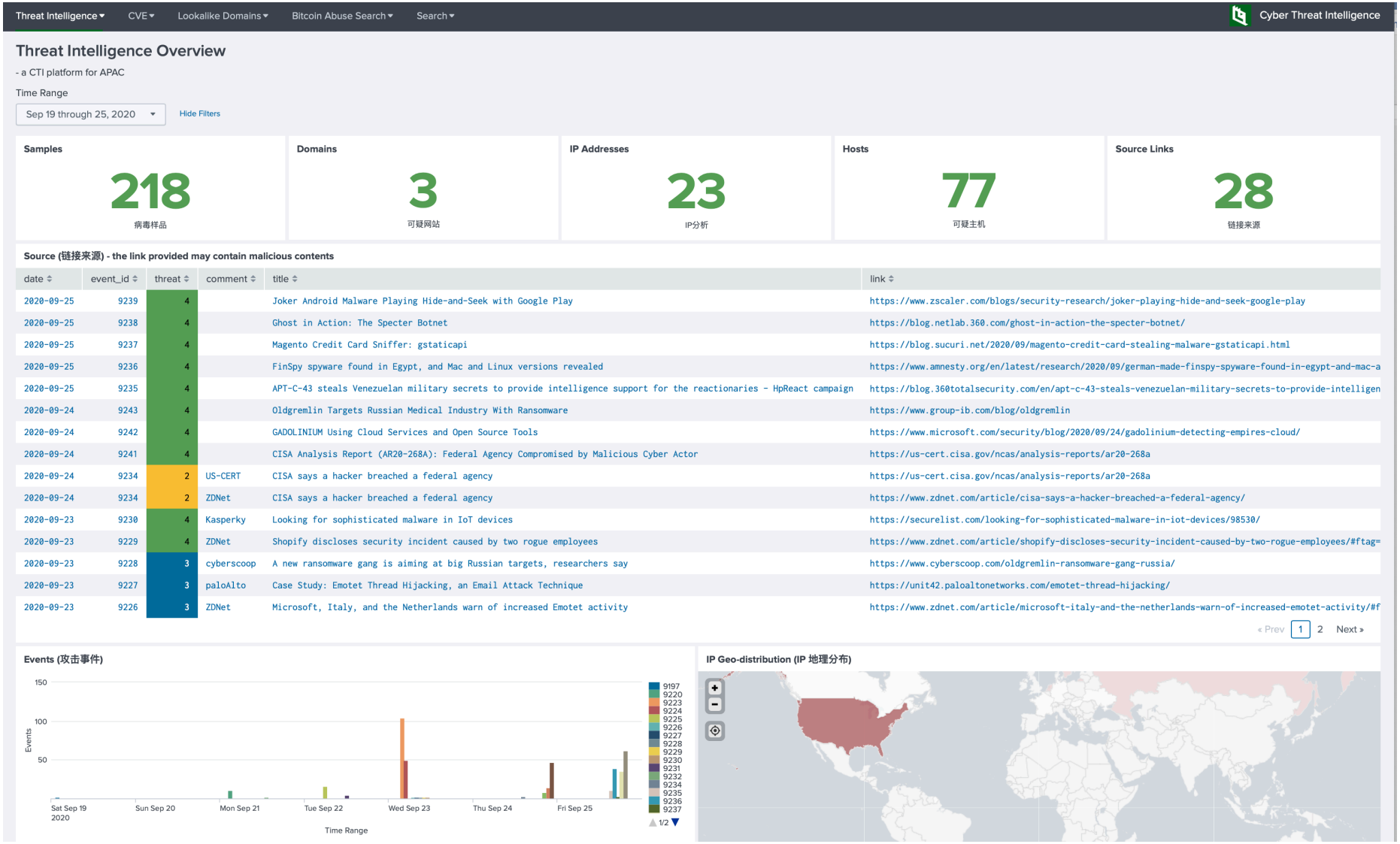
(cisp-id:9278) Sep 23, 2020
A new ransomware gang is aiming at big Russian targets, researchers say.
Medical labs, banks, manufacturers and software developers in Russia are the prime targets for a new ransomware gang that began operating with custom tools as early as March of this year, according to researchers at the security vendor Group-IB. The attackers insert their hacking tools into networks via malware downloaded through spearphishing emails, then encrypt files and hold them ransom for about $50,000, Group IB says. The group, dubbed OldGremlin, has only targeted Russian companies so far, Group-IB says. It's rare for a Russian-speaking ransomware group to aim at targets inside Russia but there are precedents, according to Group-IB senior digital forensics analyst Oleg Skulkin, who identified the hacking groups Silence and Cobalt as previous perpetrators.
https://www.cyberscoop.com/oldgremlin-ransomware-gang-russia/

(cisp-id:9277) Sep 23, 2020
Emotet Thread Hijacking, an Email Attack Technique.
Paloalto has seen significantly more Emotet malspam using a technique called "thread hijacking" that utilizes legitimate messages stolen from infected computers' email clients. This malspam spoofs a legitimate user and impersonates a reply to the stolen email. Thread hijacked malspam is sent to addresses from the original message. This technique is much more effective than less sophisticated methods, which many people have now learned to spot. The approach is more successful at convincing potential victims to click on an attached file, or to click on a link to download a malicious Word document with macros designed to infect a user with Emotet. Palo Alto Networks customers are protected from this threat because our Threat Prevention security subscription detects and prevents these types of Emotet infections.
https://unit42.paloaltonetworks.com/emotet-thread-hijacking/

(cisp-id:9231) Sep 22, 2020
CISA warns of notable increase in LokiBot malware.
CISA has observed a notable increase in the use of LokiBot malware by malicious cyber actors since July 2020. Throughout this period, CISA's EINSTEIN Intrusion Detection System, which protects federal, civilian executive branch networks, has detected persistent malicious LokiBot activity. LokiBot uses a credential- and information-stealing malware, often sent as a malicious attachment and known for being simple, yet effective, making it an attractive tool for a broad range of cyber actors across a wide variety of data compromise use cases.
https://us-cert.cisa.gov/ncas/alerts/aa20-266a

APT-C-43 steals Venezuelan military secrets - HpReact campaign
n June 2020, 360 Security Center discovered a new backdoor Pyark written in Python by the fileless attack protection function. Through in-depth excavation and trace analysis of the backdoor, we discovered a series of advanced threat actions that have been active since 2019. By invading various military institutions in Venezuela, the attackers deployed backdoor to continuously monitor and steal the latest military secrets. We named it APT-C-43 based on 360's way of naming the APT organization.
https://blog.360totalsecurity.com/en/apt-c-43-steals-venezuelan-military-secrets-to-provide-intelligence-support-for-the-reactionaries-hpreact-campaign/

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



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