# Weekly Intelligence Summary

Jul 10, 2020 (TLP: WHITE)

In the spotlight this week:

- Gemini discovered that the “Keeper” ***#Magecart*** group, which consists of an interconnected network of 64 attacker domains and 73 exfiltration domains, has targeted over 570 victim e-commerce sites in 55 different countries. Over 85% of the victim sites operated on the ***#Magento*** CMS, which boasts over 250,000 users worldwide.
- ESET has analyzed the operations of ***#Evilnum***, the APT group behind the Evilnum malware previously seen in attacks against financial technology companies. The toolset and infrastructure have evolved and now consist of a mix of custom, homemade malware combined with tools purchased from ***#GoldenChickens***, a Malware-as-a-Service (MaaS) provider whose infamous customers include ***#FIN6*** and ***#CobaltGroup***.
- The security ***#F5 BIG-IP*** hole has been described as a critical remote code execution vulnerability that can be exploited to take complete control of a system. The issue is related to the Traffic Management User Interface (TMUI) configuration utility.
- One month after security vendor ***#Group-IB*** released its own research documenting the work of a hacker known by the ***#fxmsp*** alias.

(cisp-id:8271) Jul 7, 2020

'Keeper' hacking group behind hacks at 570 online stores

Hackers also accidentally leaked more than 184,000 stolen cards through an improperly secured backend server. The Keeper gang broke into online store backends, altered their source code, and inserted malicious scripts that logged payment card details entered by shoppers in checkout forms. These types of attacks are what the cyber-security community calls ***#web-skimming***, ***#e-skimming***, or "Magecart" intrusions (named so after the first hacker group that used these tactics). In a report published today by threat intelligence firm Gemini Advisory, the company says that Keeper has been operating since at least April 2017 and continues to operate even today.

https://www.zdnet.com/article/keeper-hacking-group-behind-hacks-at-570-online-stores/#ftag=RSSbaffb68

(cisp-id:8270) Jul 9, 2020

***#WastedLocker*** Goes "Big-Game Hunting" in 2020

After initially compromising corporate networks, the attacker behind WastedLocker performs privilege escalation and lateral movement prior to activating ransomware and demanding ransom payment. The use of "dual-use" tools and "LoLBins" enables adversaries to evade detection and stay under the radar as they further operate towards their objectives in corporate environments. WastedLocker is one of the latest examples of adversaries continued use of lateral movement and privilege escalation to maximize the damage caused by ransomware. The use of "big-game hunting" continues to cause significant operational and financial damages to organizations around the globe.

https://blog.talosintelligence.com/2020/07/wastedlocker-emerges.html

(cisp-id:8268) Jul 9, 2020

More Evil: A deep look at Evilnum and its toolset

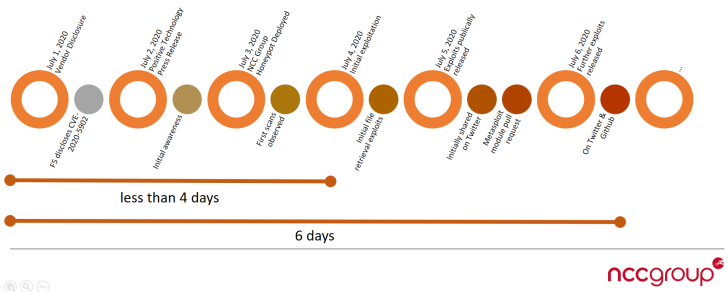
ESET has analyzed the operations of Evilnum, the APT group behind the Evilnum malware previously seen in attacks against financial technology companies. While said malware has been seen in the wild since at least 2018 and documented previously, little has been

published about the group behind it and how it operates. The group's targets remain fintech companies, but its toolset and infrastructure have evolved and now consist of a mix of custom, homemade malware combined with tools purchased from Golden Chickens, a MaaS provider whose infamous customers include FIN6 and Cobalt Group.
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

(cisp-id:8256) Jul 7, 2020
Feds indict ***#fxmsp*** in connection with million-dollar hacking operation
The U.S. Department of Justice has charged a man with hacking-related crimes as part of an investigation into a group of foreign scammers accused of targeting more than 300 organizations throughout the world. Prosecutors in the Western District of Washington charged Andrey Turchin, who resides in Kazakhstan, with five felony counts in connection with a year-long fraud effort. Last known to be in Kazakhstan, Turchin allegedly sold remote access hacking tools on cybercriminal forums, typically charging tens of thousands of dollars for access to data that would cost victims tens of millions of dollars. Turchin went by a series of aliases, including "fxmsp," according to the Justice Department. He was initially charged in December 2018, though the indictment was kept under seal until Tuesday, one month after security vendor Group-IB released its own research documenting the work of a hacker known by the "fxmsp" alias.
https://www.cyberscoop.com/fxmsp-andrey-turchin-indictment-fraud-stolen-data/

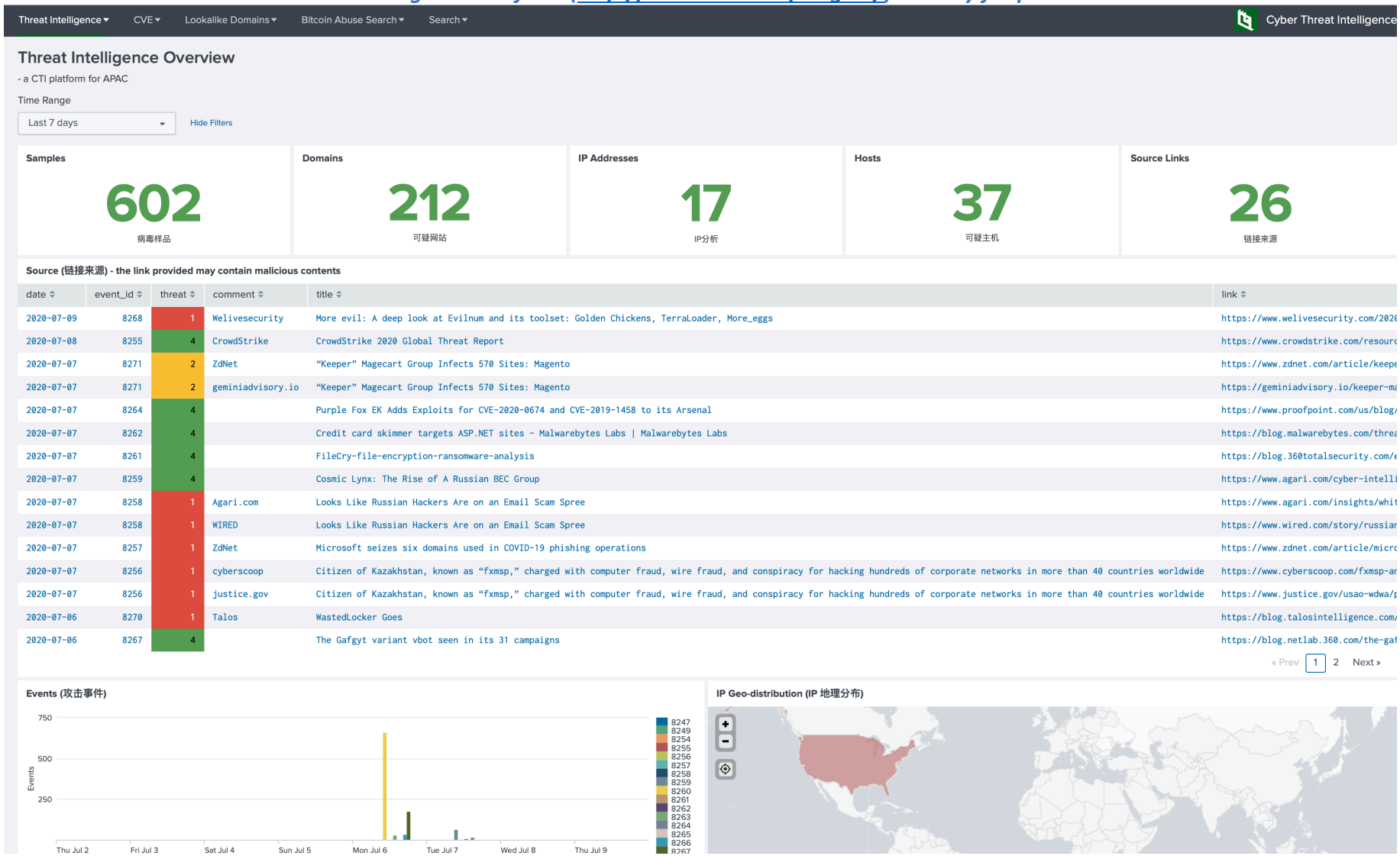
(cisp-id:8263) Jul 6, 2020
***#BIG-IP*** Vulnerability Exploited to Deliver DDoS Malware
CVE-2020-5902 was disclosed on July 1st, 2020 by ***F5 Networks*** in K52145254 as a CVSS 10.0 remote code execution vulnerability in the Big-IP administrative interface. By July 3rd, 2020 NCC Group observed active exploitation. This blog is a summary of what we know as the situation develops. Hackers continue to exploit the recently patched BIG-IP security flaw and they have plenty of potential targets as researchers have identified thousands of vulnerable systems. The security hole has been described as a critical remote code execution vulnerability that can be exploited to take complete control of a system. The issue is related to the Traffic Management User Interface (TMUI) configuration utility. An attacker who has access to this utility *can exploit the weakness to create or delete files, disable services, intercept data, and run arbitrary code or commands*. Proof-of-concept (PoC) exploits and technical information were made public for CVE-2020-5902 shortly after its disclosure and the first exploitation attempts were observed soon after. The vulnerability is easy to exploit, and experts have pointed out that the entire exploit fits in a tweet.
https://www.securityweek.com/big-ip-vulnerability-exploited-deliver-ddos-malware

Timeline from disclosure to exploitation for CVE-2020-5902




Source From: Nccgroup

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




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