Weekly Intelligence Summary

Jun 5, 2020 (TLP: WHITE)

In the spotlight this week #ransomware #O365:

- In our 15/6 Summary we said: Maze ransomware has targeted organizations on Fortune 500s (#HK). This week we found #HK business entities: Bossini and City Super seems infected with #MAZE and #Netwalker (also mentioned in our 28/5 Summary) and part of their data was released in the dark web.
- Not only business entities, DopplePaymer ransomware gang says it breached one of NASA's IT contractors - Digital Management Inc. It is unclear how deep inside DMI's network the DopplePaymer gang made it during their breach.
- Abnormal Security disclosed their findings on Office 365 phishing baits. Customers are targeted by a campaign using messages and phishing landing page camouflaged as notifications sent by their organization to update the VPN configuration.
- Protect Your System my friend: After getting access, [ransomware actors] used ***mimikatz*** to dump credentials and ***psexec*** for lateral movement. ***Advanced Port Scanner*** and ***Advanced IP Scanner*** were used for network recon. Additionally, a ***powershell script*** was implanted that ***stops AV***, ***delete backups***, and ***modifies local account passwords*** to prepare the system for encryption. The group also left behind installations of ***Putty***, ***WinSCP***, a Go ***RAT***, and ***PowerShell Empire penetration-testing tool.*** #RedTeam

(cisp-id:8081) Jun 4, 2020

Protect Your System Amigo

There hasn't been much chatter about Mespinoza ransomware or "Protect Your System Amigo" Pysa crew recently, but they are successfully landing their ransomware.

We found 20 instances of victim data being published online. After getting access, Pysa used mimikatz to dump credentials and psexec for lateral movement. Advanced Port Scanner and Advanced IP Scanner were used for network recon. The group also left behind installations of Putty, WinSCP, a Go RAT, and PowerShell Empire penetration-testing tool.

https://medium.com/@ransomleaks/protect-your-system-amigo-2520bdfccbba

(cisp-id:8080) Jun 4, 2020 (Apr 28, 2020)

"黑玫瑰露西"回归-演变为勒索软件: Lucy Loader.

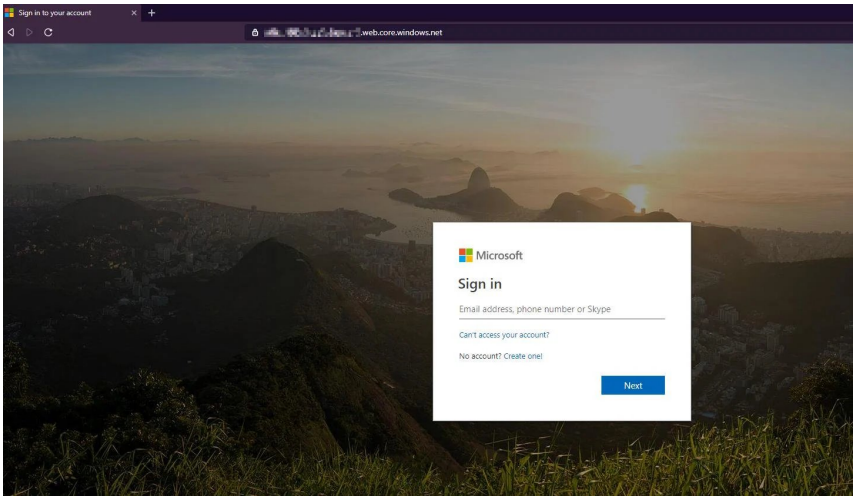
Ransomware attacks have been a part of the security landscape for a long time. We are familiar with infamous malware such as CryptoLocker, WannaCry and Ryuk, all of which have caused enormous damage to organizations and private assets globally. And while ransomware has just started to take its first steps in the mobile world, it's evolving fast as malware developers and attackers apply the experience, they have gained to create disruptive mobile ransomware attacks. An example is the 'Black Rose Lucy' malware family, originally discovered in September 2018 by Check Point. And now, nearly two years later, it is back with new ransomware capabilities that allow it to take control of victims' devices to make various changes and install new malicious applications.

https://research.checkpoint.com/2020/lucys-back-ransomware-goes-mobile/

https://www.freebuf.com/articles/terminal/236081.html

(cisp-id:8078) Jun 3, 2020
Ransomware gang says it breached one of NASA's IT contractors.
DopplePaymer ransomware gang claims to have breached Digital Management Inc. (DMI), a major US IT and cybersecurity provider, and one of NASA IT contractors. According to the company's press releases, DMI's customer list includes several Fortune 100 companies and many government agencies, among them NASA. It is unclear how deep inside DMI's network the DopplePaymer gang made it during their breach, and how many customer networks they managed to breach. Three DMI spokespersons did not answer phone calls from ZDNet seeking comment for this article. The archives include everything from HR documents to project plans, as can be seen from a screenshot ZDNet took of one of the files. Employee details included in these files matched public LinkedIn records.
https://www.zdnet.com/article/ransomware-gang-says-it-breached-one-of-nasas-it-contractors/

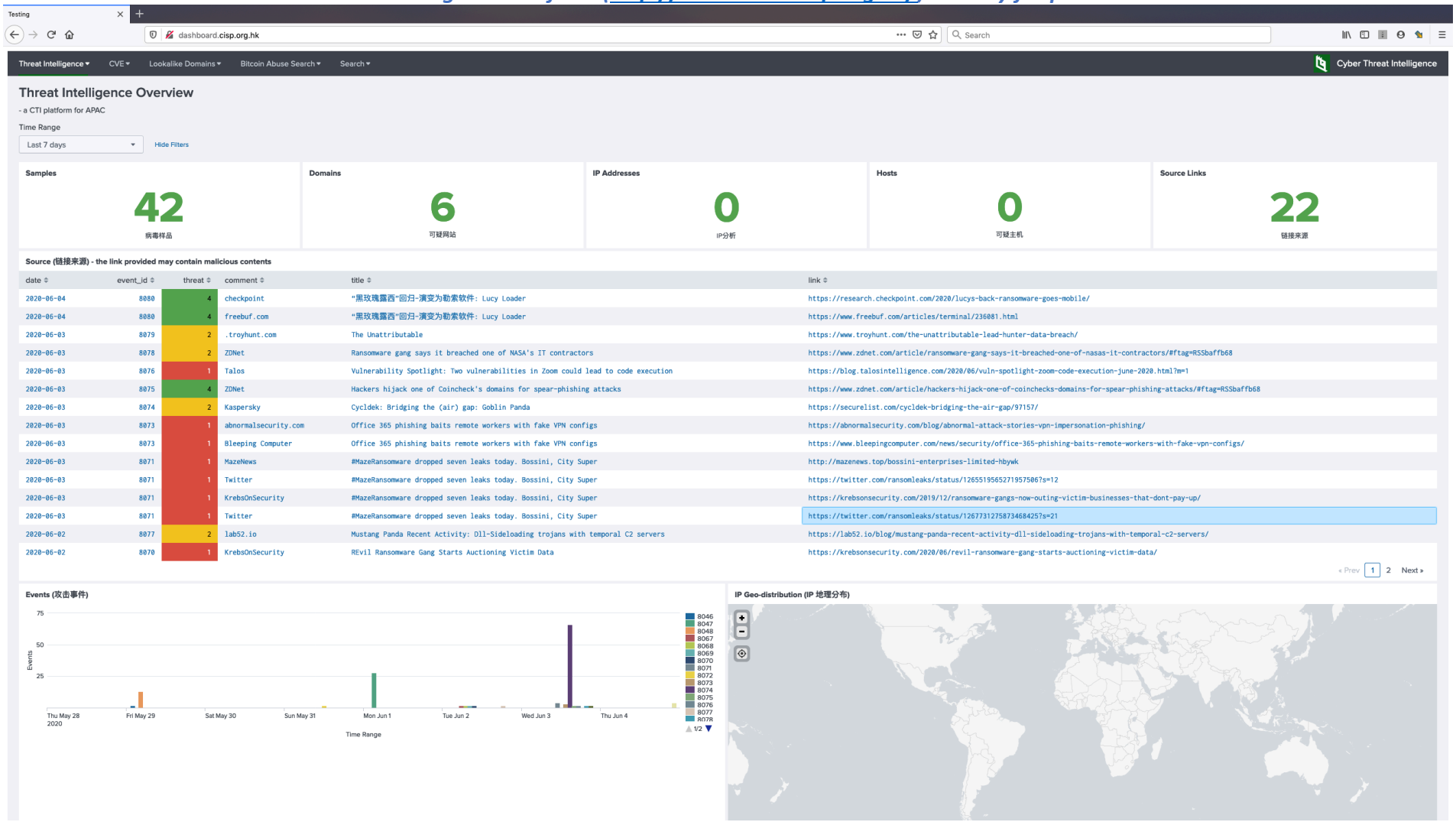
(cisp-id:8073) Jun 3, 2020
Office 365 phishing baits remote workers with fake VPN configs.
Microsoft Office 365 customers are targeted by a phishing campaign using bait messages camouflaged as notifications sent by their organization to update the VPN configuration they use to access company assets while working from home. The phishing emails impersonating VPN configuration update requests sent by their company's IT support department have so far landed in the inboxes of up to 15,000 targets according to stats from researchers at email security company Abnormal Security. These phishing messages are a lot more dangerous because of the huge influx of employees working remotely and using VPNs to connect to company resources from home for sharing documents with their colleagues and accessing their orgs' servers.
https://www.bleepingcomputer.com/news/security/office-365-phishing-baits-remote-workers-with-fake-vpn-configs/
https://abnormalsecurity.com/blog/abnormal-attack-stories-vpn-impersonation-phishing/



Phishing landing page hosted on web.core.windows.net

(cisp-id:8071) Jun 2, 2020
A newly created twitter account @ransomleaks disclosed ransomware incidents. #MazeRansomware dropped seven leaks today. That's a record high. Here's the victims w/revenue. Bossini(<1m) and #NetWalker is threatening to #leak data from #breach http://citysuper.com.hk in 6 days. City Super is "Hong Kong's first-of-its-kind Mega Lifestyle Specialty Store"
https://twitter.com/ransomleaks/status/1265519565271957506
https://twitter.com/ransomleaks/status/1267731275873468425

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



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