Cyber-Intelligence Report

This cyber-intelligence product is produced by David Swan. Collection of information is in accordance with guidelines provided by clients. It contains 'observations', meaning headlines and links to information published online. It *MAY* contain comments and analysis. It is copyright ©David Swan 2022. It MAY be circulated.

If this report does not meet your requirements, is in error or if you need additional information and/or analysis, please contact David Swan at DSC.Ops.Vulcan@gmail.com

Cyberwarfare: Russia vs Ukraine (18)

This report contains selected cyber-security information from 28th October to 18th November 2022.

1. Russia has been ramping up cyber operations including production of new malware and the creation of new cyber-criminal groups. One new group probably hacked the Empire Company (Sobey's). The BBC published a report on U.S. Cyber Command's Hunt Forward Operation in Ukraine.

2. Russian 'Courses of Action' for cyber forces, including allies such as 'patriotic', mercenary, and domestic criminal hackers are *assessed* as:

> **Ongoing**: Russian cyber forces, including allied forces, have launched a series of cyber attacks against **both strategic targets and general targets** as well as vulnerable governments.
>
> **Worst Case Scenario**: President Putin decides to focus Russia's cyber attacks on one country (such as Canada) or a small group of vulnerable countries. *Assessed as UNLIKELY.*
>
> **Best Case Scenario:** Russia agrees to cease or is forced to cease offensive cyber operations. *Assessed as VERY UNLIKELY.*

Russia

3. **Russia Ramping Up Cyber-Operations:** Analysis from the U.S. Department of Justice's Financial Crimes Enforcement Network reveals that Russian actors comprised roughly three-quarters of recorded ransomware incidents during the latter portion of 2021. "Officials attributed 594 of the ransomware-related activities recorded between July and December 2021 to Russia-linked actors, out of a cumulative 793 reported to the agency during that time frame.[1] Analysts Comment: That report is based on *reported* ransomware attacks. It is likely that only 15 to 25 percent of cyber-attacks are reported, depending on state jurisdiction within the U.S. The basis for identifying the attackers was: "variants were identified in open source information as using Russian-language code, being coded specifically not to attack targets in Russia or post-Soviet states or as advertising primarily on Russian-language sites".[2]

4. **New Russian Cyber-Criminals – Black Basta:** Note: This is the group that

1 Source: NextGov: Russia Linked to Nearly 75% of Late 2021 Ransomware Attacks, Per Analysis
2 Ibid.

Bleeping Computers believes hacked the Empire Company (Sobey's).[3] Evidence suggests that this organization has been developing since February 2022. It emerged in April as a ransomware as a service (RaaS)organization. Palo Alto Networks reports: Black Basta affiliates have been very active deploying Black Basta and extorting organizations since the ransomware first emerged. Although the Black Basta affiliates have only been active for the past couple of months, based on the information posted on their leak site, they have compromised over 75 organizations at the time of this publication. ... The Black Basta operator(s) use the double extortion technique, meaning that in addition to encrypting files on the systems of targeted organizations and demanding ransom to make decryption possible, they also maintain a dark web leak site where they threaten to post sensitive information if an organization chooses not to pay ransom. At least 20 victims were posted to its leak site in the first two weeks of the ransomware's operation. Based on multiple similarities in tactics, techniques and procedures (TTPs) - victim-shaming blogs, recovery portals, negotiation tactics, and how quickly Black Basta amassed its victims - that the Black Basta group could include current or former members of the Conti group.[4]

5. Victims have reportedly been hit in countries around the world including the United States, UK, India, Canada, Australia, New Zealand, and UAE.[5] Black Basta is primarily targeting the industrial, retail, and real-estate sectors. Their attack vectors include malspam, where an email with a business inquiry invites the recipient to open an attachment, and insider threats. In the second case, malicious actors turn to darknet forums to look for insiders.[6]

6. **Russia's ongoing cyber-attacks**: Cybersecurity company Proofpoint reported on 3rd November that a threat actor it tracks as TA569 appears to be behind an attack on hundreds of regional and national news websites in the United States. The sites are now delivering malware. More than 250 news sites are impacted, including in Boston, New York, Chicago, Washington DC, Miami, Palm Beach and Cincinnati. The actual number of victims could be higher.[7] TA 569 has been active since at least late in 2016. ProofPoint described TA569 as: "TA569 is a traffic and load seller known for compromising content management servers and injecting and redirecting web traffic to a social engineering kit."[8]

7. Other ongoing cyber attacks include:

> A. **Emotet Botnet:** This malware began life as a banking Trojan created by a Ukrainian/Russian criminal hacker group. The hacker group was identified and arrested in 2021. In November 2021 the 'botnet returned "evolving into spamming and malware delivery – are now using it to target credit card information stored in the Chrome web browser." ... In a March threat index, Check Point researchers put the Windows software nasty at the top of its list as

3 Source: Bleeping Computer: Canadian food retail giant Sobeys hit by Black Basta ransomware
4 Source: Palo Alta Newworks – Unit 42: Threat Assessment: Black Basta Ransomware
5 Source: Tripwire by Fortra: Black Basta ransomware - what you need to know
6 Source: CyberInt reported in CyberNews: Black Basta: a new ransomware group or a Conti faction?
7 Source: Security Week: Over 250 US News Websites Deliver Malware via Supply Chain Attack
8 Source: ProofPoint: The First Step: Initial Access Leads to Ransomware

the most widely deployed malware, menacing or infecting as much as 10 percent of organizations around the globe during the month."[9] researchers noted a few months ago that the botnet 'went on a hiatus'. There are now reports that the Emotet malware-delivery botnet is back quickly ramping up the number of malicious emails it's sending and sporting additional capabilities, including changes to its binary and delivering a new version of the IcedID malware dropper. Emotet is again fully functional, acting as a delivery network for other malware families.[10] The botnet was activated daily between November 2nd and 11th in what we *assess* as test runs. Emotet is *assessed* as operationally ready to start new campaigns.

B. Russian hacker group Killnet claimed a cyber attack on the FBI website. According to Newsweek: "The hacking group Killnet shared a post on its Telegram page on Monday flagging an "attack" on the law enforcement resources site for the FBI. The message included a photo of what looked to be a failed attempt to enter the FBI site." Cybersecurity organizations are agreed there was negligible impact on the FBI."[11]

C. Planting malware. Apparently thousands of smartphone applications in Apple and Google's online stores contain computer code developed by a technology company, Pushwoosh, that presents itself as based in the United States, but is actually Russian. On social media and in U.S. regulatory filings, however, it presents itself as a U.S. company, based at various times in California, Maryland and Washington, D.C., Reuters found. According to company documents publicly filed in Russia and reviewed by Reuters, Pushwoosh is headquartered in the Siberian town of Novosibirsk, where it is registered as a software company that also carries out data processing. It employs around 40 people and reported revenue of 143,270,000 rubles ($2.4 million) last year. Pushwoosh is registered with the Russian government to pay taxes in Russia. A number of U.S. Federal departments, including the U.S. Army ordered Pushwoosh applications removed.[12]

Ukraine

8. Ukraine: Ukrainian operational security remains tight on their offensive activity with no information being released. There are indications that defensive operations continue as multiple criminal hacking operations have been shut down. For example: On November 13th Ukrainian police 'dismantled' a transnational fraud group that was harvesting €200 million per year. Investors were tricked into initiating a series of fake investments. The gang established its offices and call centers, employing more than 2,000 people. Ukrainian police were supported by law enforcement in Albania, Finland, Georgia, Germany, Latvia and Spain.[13]

9 Source: The Register: Emotet reestablishes itself at the top of the malware world
10 Source: The Register: Notorious Emotet botnet returns after a few months off
11 Source: Newsweek: Russian Hackers Claim Cyber Attack On FBI Website
12 Source: Business Insurance: Russian software disguised as American finds its way into US Army, CDC apps
13 Source: Security Affairs: Ukraine Police dismantled a transnational fraud group that made €200 million per year

9. **U.S. Military's "Hunt Forward" Operations:** The next two paragraphs are rewritten from a BBC article. "Since 2014, Ukraine has witnessed some of the world's most significant cyber-attacks, including the first in which a power station was switched off remotely in the dead of winter. ... By late last year, Western intelligence officials were watching Russian military preparations and growing increasingly concerned that a new blizzard of cyber-attacks would accompany an invasion, crippling communications, power, banking and government services, to pave the way for the seizure of power. ... In early December last year, a small US military team led by a young major arrived in Ukraine on a reconnaissance trip ahead of a larger deployment. But the major quickly reported that she needed to stay. ... She looked at the situation and told me the team wouldn't leave, Maj Gen William J Hartman, who heads the US Cyber National Mission Force, told the BBC. ... The US military Cyber Command wanted to discover whether Russian hackers had already infiltrated Ukrainian systems, hiding deep inside.

10. Most of their work has been battling state-hackers from China and North Korea but Russia has been their most persistent adversary. ... This means a new role for the US military, whose teams are engaged in "Hunt Forward" missions, scouring the computer networks of partner countries for signs of penetration. ... The US teams say they share what they find to allow the local partner to eject Russians (or other state hackers) rather than do it themselves. ... They also use commercial tools so that local partners can continue after the mission is over. ... Hunt Forward missions are classed as "defensive" but Gen Paul Nakasone, who leads both the military's Cyber Command and the National Security Agency confirmed offensive missions have also been undertaken against Russia in the wake of the invasion of Ukraine."[14]

11. **Support to Ukrainian Cyber Operations**: Reuters reports: The German government has earmarked an extra 1 billion euros ($1.03 billion)from its 2023 budget to support Ukraine, with money allocated to defending against Russian cyberattacks and collecting evidence of war crimes, a document showed.[15] This is considered a political win for the Green Party in Germany as that party are the most vocal supporters of Ukraine.

Analysis

12. As we correlate malware with hackers and hacker groups with sponsor nations, we are observing deployments of high capability malware supported by seasoned criminals. A large percentage of those criminals are sponsored or at least protected by nations. The hack of the Empire Group and *probably* Maple Leaf Foods are indicators of major cyber attacks that Russia is inflicting on the rest of the world.

---

14 Source: BBC: Inside a US military cyber team's defence of Ukraine
15 Source: Reuters: Germany allocates extra 1 bln euros to Ukraine cyber-defence, documenting war crimes