Curious tale of 8.t used by multiple campaigns against South Asia

Thursday 3 October 15:00 - 15:30, Red room

Niranjan Jayanand (Microsoft)
Ivan Macalintal (Microsoft)
Debalina Ghosh (Microsoft)

This presentation will cover the long-running attack campaigns targeting South Asian officials mainly working in the government, oil, media and maritime sectors as well as defence contractors, universities (particularly those with military research ties) and legal organizations. The main motivation behind these attacks is espionage aligned with commercial and South China Sea issues for intellectual property theft and military espionage.

Attackers use multi-stage attack techniques to target their victims during their campaigns. During the reconnaissance stage, they collect lots of information such as the software and applications that are vulnerable at the customer end. Over the past few years, attackers have been using poisoned Microsoft Office documents as one of their preferred infection vectors for cybercrime and cyber espionage attacks. It doesn't take long for malware authors to integrate novel techniques into their own exploit kits and attack ordinary users. Attackers quickly adopt most of these application CVEs.

In the campaigns we analysed, it was identified that multiple APT groups (namely Leviathon, Goblin Panda, Winnti and Sidewinder) targeted South Asian countries using the Microsoft Office vulnerabilities CVE-2017-11882, CVE-2017-0199 and CVE-2017-8759. From fellow researchers' APT research, it was also identified that a unique object dimension present in RTF phishing files was weaponized with CVE-2017-11882 and CVE-2018-0802, which appear to be utilized by numerous Asian APT groups. The identified RTFs all share a unique object height and width, which determine how the object will be rendered in Microsoft Word. We used this to expand our research to track APT groups.

Once the victim executes the poisoned Microsoft Office files, the shellcode that decrypts the final payload in memory was identified to use one constant file name, '8.t', across all the campaigns. Some of the identified payloads are NewCore RAT, Hawkball backdoor, Fucobha, QCRat, PlugX, htpRAT and an unnamed RAT. Most of these remote administration tools relied on the DLL side-loading technique to survive on reboot. It is very rare to see possibly different APT groups using the same shellcode name and two different shellcode decryption logics to drop and execute final RAT payloads on victim machines, across different identified APT campaigns. It was also identified that attackers came back to target almost the same victim organizations in South Asian countries over this time. At a certain time, the APT groups likely had an infrastructure overlap.

Attackers continued using the same trends and traits with minimum modification to target the same victims, regions and sectors, which makes us belief that they may have shared TTPs, code and infrastructure to steal intellectual data from victim organizations. Many filenames and attacker command-and-control domains collected during the investigation used themes related to the victim country current affairs or organizations.

Niranjan Jayanand

Niranjan Jayanand has over 11 years of experience in anti-malware and security companies *including Symantec* and *McAfee* and has recently joined *Microsoft*. Niranjan is an experienced principal threat intelligence analyst with sound knowledge of threat group tracking, reverse engineering, Yara , generic antivirus signature creation and threat report writing for customers. He has authored over 60 proactive APT reports on attacks hitting the MENA region and South Asian countries. He has good experience working on PRC origin attacks and Iranian groups. Among the attacks investigated , most of them were identified when the attack was on going and customers were alerted at the earliest. In the past Niranjan has worked on multiple customer escalations on outbreaks that have infected many machines, and helped them remediate infections. In his free time, Niranjan loves travel, spending time with his family and pets. He is very active with a number of charity groups in South India and finding out ways on how he can help others.

Debalina Ghosh

Debalina Ghosh is a Threat Intelligence Analyst at *Microsoft* and is based out of Hyderabad. She graduated in 2018 and has been a part of the Threat Intel team ever since March 2019. Debalina has a background in the offensive side of security, and holds a GPEN certification from SANS, she also holds eCPPT and eJPT certification from eLearnSecurity. Debalina currently works on telemetry hunting and attribution of threat actors. She hunts for new TTPs across various online platforms and collects sources for the same. During her time at university Debalina led the Cyber Security Club for two years. She plays a lot of Capture the Flag (CTF) competitions and won the Winja Capture the Flag, which was held at NullCon. She also won the BlackHat Asia Scholarship 2018, which was hosted in Singapore. She has also participated at HackIM CTF NullCon and was ranked in the TOP 20. In her free time, Debalina travels and likes to spend time with animals.

Ivan Macalintal

Ivan Macalintal has spent more than 16 years in the anti-malware and security industry and progressed from an-timalware engineer, analyst and researcher roles to founding and leading operations and threat research teams as well multiple high-impact projects, processes and services for global industry partners and customers, in *Trend Micro* for more than a decade, and now in *Microsoft* for more than four years.

Ivan is passionate about:

1) Threat analysis and research, connecting the dots and spotting the needles in the haystack of threat intelligence from advanced persistent threats, targeted attacks, cybercrime campaigns and other threats targeting data confidentiality, integrity and availability;

2) Reverse-engineering, static and dynamic code analysis, Internet forensics, open source intelligence;

3) Industry, partner and customer engagements;

4) Global and regional cross-functional and cross-cultural project and people management for anti-malware, cyber-threat solutions research, planning, and deployment;

5) Correlation and consolidation of big data to protect customers and to further research new emerging threats.

Ivan has published numerous impactful and newsworthy blog articles and presented at various industry conferences: Virus Bulletin, Association of Antivirus Asia Researchers (AVAR), the High Technology Crime Investigation Association (HTCIA), B-Sides, Digital Crimes Consortium (DCC), Microsoft TechEd North America and the Microsoft Security Response Alliance (MSRA) summit, and has been a well-travelled SME, consultant and resource for management and executive teams for customer and threat-marketing related projects and goals.

During his free time, he leads efforts in diversity and inclusion and is involved in projects for non-profit community building. He is also starting to write mystery novels, forever searching for the perfect cup of coffee and enjoys simply spending time with family and friends to 'make a life, not just a living'.

BACK TO VB2019 PROGRAMME PAGE

Other VB2019 papers

Keynote: Nexus between OT and IT threat intelligence
Selena Larson (Dragos)

Exploring Emotet, an elaborate everyday enigma
Luca Nagy (Sophos)

Call the shots! Let's fight crime together
Speaker TBA (NHTCU)