Dragon Advance Tech

Suite 701-702, 7/F, Shun Feng International Centre, No. 182 Queen's Road East, Wanchai, Hong Kong
Phone +852 2868 6182 Email: admin@dragonadvancetech.com

Cybersecurity Alert : Ransomware leverage RDP in attacks

Author: Frankie Li
Chief Security Analyst - DAT

Frankie Li is the Chief Security Analyst at Dragon Advance Tech (http://Dragonadvancetech.com). He is a speaker in various security conferences: US Blackhat, Cyber Security Consortium (HK), HITCON (Taiwan), (ISC)2 Security Congress (APAC), CyberCrimeCon 2018 (Russia) and High-Tech Crime Investigation Association (HTCIA, APAC) and Founder of Dragon Threat Labs (http://dragonthreatlabs.org), DragonCon (http://dragoncon.hk)

TLP:GREEN

Hong Kong SMEs' Internet facing RDP connections are subject to brute force attacks. Compromised systems may be planted with ransomware after sufficient data has been collected.

Many SMEs in Hong Kong their IT support to external IT service companies Those ad hoc IT teams tend to deliver their IT maintenance services through RDP (Remote Desktop Protocol) to the clients' computers from their Internet facing devices. We observed that many Internet facing RDP connections are subject to brute force attacks and compromised systems were planted with ransomware after sufficient data has been collected.

Firewalls and anti-virus solutions are insufficient and ineffective in protecting against these threats, especially if they are mis-configured. We advise Hong Kong SMEs to put additional cybersecurity countermeasures such as security incident monitoring to defend their critical computer networks and systems and identify the source of the attacks. Otherwise, recurring attacks might happen.

Recently, the Computer Security Incident Response Teams from Dragon Advance Tech observed several incidents of ransomware reports from Hong Kong SMEs during September and October 2018. Coincidentally, in the same period of *2017*, HKCERT also identified 18 infection cases[1] of the ransomware called Crysis from domestic victims including a school.

The Crysis ransomware was identified by Malekal_morte[2], Trend Micro[3] in early 2017 and further confirmed by Bleeping Computer in August 2017. A detailed reverse engineering report of the ransomware was published in November 2017 by Panda Security[4]. Lawrence Abrams of Bleeping Computer provided a general description of the ransomware - "When the ransomware is installed, it

[1] https://www.hkcert.org/my_url/en/blog/17110901

[2] http://forum.malekal.com/viewtopic.php?t=54445&start=

[3] https://blog.trendmicro.com/trendlabs-security-intelligence/brute-force-rdp-attacks-plant-crysis-ransomware/

[4] https://www.pandasecurity.com/mediacenter/src/uploads/2017/11/Ransomware_Crysis-Dharma-en.pdf

will scan the computer for certain file types and encrypt them. The encrypted file will append with an extension in the format of *.id-[id].[email].arena*"[5].

In some of our investigated cases, the extension changed to *.id-[id].[email].bip*.

Normally, ransomware is infected through spamming emails, drive-by-downloads, malvertisment with exploit kits or self-propagation like WannaCry. Typical ransomware authors will try to distribute the ransomware to large number of potential victims spontaneously for maximizing their financial gains. Usually these ransomwares do not require a persistence mechanism.

However, these Crysis cases are different because this ransomware was usually *planted manually* onto the victim systems through RDP access. In one of the cases we investigated, the attacker first brute-forced the RDP login from a Swedish IP address, planted the malware together with mimikatz (a password collection utility) and generated some text files with names like "good.txt", "IP.txt", "servers.txt", "settings.ini" and "credentials.txt" before launching the ransomware. We cannot verify how much and what kinds of information have been harvested by the attackers because the log files were also encrypted by the ransomware. We also found that this ransomware uses several persistence methods to ensure it will start up on the next computer reboot.

We believe the victims' computing systems were actually *being hacked first*, and after gaining initial access, the attacker collected more information during their *lateral movements* and finally launched the ransomware for financial gain.

This is not common in most ransomware cases.

To the best of our knowledge, most of these cases are not being investigated and the victims are usually SMEs or NGOs. These organizations have a limited budget to appoint a cybersecurity professional, and some even do not have a full time IT staff to handle their IT support duties. Hence, ad hoc or out-sourced IT staff are appointed to perform maintenance remotely, usually through RDP. These out-sourced IT staff tend to use the same (and usually weak) passwords for accessing all their clients' internet-facing devices, such as routers or firewalls. A forwarding RDP rule will then be created to access one of the client's always-on machines, usually a server (such as a file server), which then allows the IT staff member to connect to the client's network for performing their maintenance tasks.

The SME clients have no knowledge on how these RDP accounts are created, nor the weak passwords used for RDP and routers/firewalls.

Hong Kong SMEs' management has a common misconception that if they have purchased a firewall and their desktop machines are installed with anti-virus solutions, then their computer networks and systems will be secured.

HKCERT has published prevention and mitigation guidelines[6] on protection against ransomware.

[5] https://www.bleepingcomputer.com/news/security/new-arena-crysis-ransomware-variant-released/

[6] https://www.hkcert.org/ransomware.hk/ransomware-basic.html

Dragon Advance Tech

Suite 701-702, 7/F, Shun Feng International Centre, No. 182 Queen's Road East, Wanchai, Hong Kong
Phone +852 2868 6182 Email: admin@dragonadvancetech.com

To protect against attacks like Crysis or attackers who brute-force open Internet facing remote administration services (such as: RDP, TeamViewer or VNC), we advise Hong Kong SMEs to put in additional countermeasures, such as proper configuration of security technologies and security incident monitoring, to their network protection. Internet facing devices should be protected by strong passwords, and with all logging functions turned on. Internet-accessible RDP services should be turned off unless they are necessary. In case RDP is absolutely necessary, it should be made available on an on-demand basis (i.e. turn it on only on request and shut it down immediately after remote administration works are completed).

If any security incidents happen, appoint a qualified cybersecurity professional as quickly as possible to review and contain the attacks, and/or implement a continuous security monitoring service for better protection because:

"IT CAN HAPPEN TO ANYONE AND MAY HAPPEN AGAIN"