Threat intelligence: Advisory 103 (I&W, CTI) December 13th 2019

threatintelligence@onnetservices.io

Dear all,

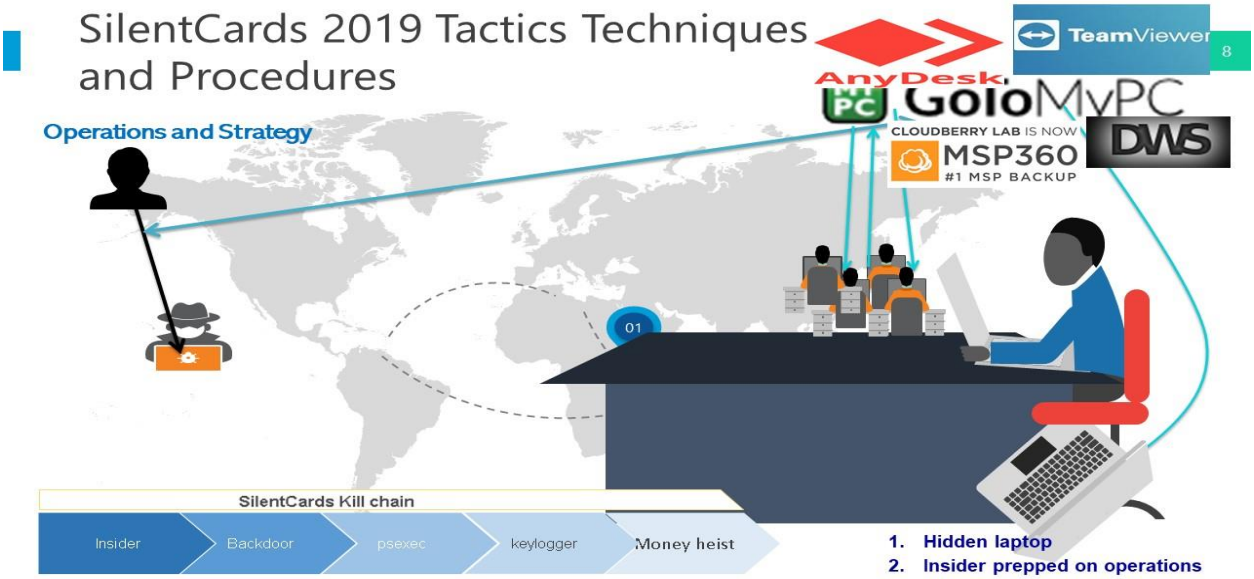
Blessed Jamhuri day.

Last month, a takedown of one of the largest Cyber threat groups in Eastern and Central was executed and the group was officially terminated.

The groups name is Forkbombo which was reborn after the Cartel split up in 2017. With the take down of this group in borders of Rwanda, we have noticed aggressive operations by rival threat group, SIlentCards, to increase their revenue threshold from October 2019 to date.

From our Data Analytics we can tell the SilentCards threat group have managed to steal more than 2Bs around East Africa from 2018 to 2019 and was observed by our partner company, GroupIB during a heist in Uganda and Kenya, and thus currently ranked top 10 Financial Threat groups in the world and Top 3 in Africa. The report from GroupIB Europe can be read here.

With SilentCards aggressive attacks, we have collected their current Tactics, Techniques and Procedures as shown below which has been updated with new tools detected i.e ***DW Agent, CloudBerry Remote Assistant and Shell443.exe(SeaDuke)***



As usual, insiders are a biggest part of successful operations as a major (TTP) Tactics Techniques and Procedures which they haven't successfully abandoned. This group had around 20 members with around 12 hackers. Five members of the hacker group left on July 2019 due to internal financial conflict followed by one major partner of the group this September 2019.

The five operators formed a new group with almost same tactics, that we have codenamed as RuiruShepherds. We have noticed the group is currently practicing new methods of writing backdoors and use of Metasploit during initial penetration.

SilentCards major leader who left the threat group is a former police officer, and the former leader of Forkbombo Cyber Cartel. He is currently busy forming a new group, that OnNet is tracking as The_Consultants and is actively exploiting backdoors established by SilentCards over the year, 2019.

Holidays are prime season for intrusions, sometimes support and security is lax and high volumes of transactions are expected. Having a downtime during this duration can result to great losses of revenue. Security and Intelligence are investments of the future, sometimes those investments take longer to pay off, and sometimes it is challenging to demonstrate the value in a world where unknown catastrophes are avoided. It’s always advisable to learn from other misfortunes than yours.

Due to the aggressiveness of the four local groups, GrapZone, TheConsultants, SilentCards and West-African group Corezeta, OnNet has decided to share with you, the customer, PEs (Portable Executables) caught around Kenyan Financial infrastructure. We have also shared APT PEs caught and attributed to Western, Europe and Asian governments during intrusion into Government of Kenya network.

See as below:

http://onnetservices.io/PEsForShares/TheThreatGroups2019Defend/

To familiarize with international groups, https://attack.mitre.org/groups/

A Note from OnNet CTO

Good afternoon,

Thank you for helping us defend you this year, as always, your mission is ours.

As adversaries mutate and multiply and others are terminated, the good guys will always prevail.

On this advisory NO. 103, we have published the latest tools used by the major groups locally and we have also uploaded toolkits seen in the GoK infrastructure this year. Also we have added toolkits from a WestAfrican group we call Corezeta that works with Nigerians in Kenya to run Visa operations and sometimes Ransomware.

Kindly look into them, download via Linux and reverse them, collect signatures and configure them into your reporting tools e.g SIEMs and if you spot any indicators, report it immediately to management as you remediate. Keep searching for these signatures in your infrastructure, we hope no-one will be robbed this Holiday. SilentCards cyber gang is the biggest now and with the other main group terminated in Kigali, they have become aggressive, set out to pick new targets to enlarge fast and grow their revenue. As blueteam we operationalize intelligence, we have also outed their toolkits and infrastructure to authorities here and abroad and even later responded to major heists with the same tools because someone failed to updated their infrastructure. Understanding your infrastructure to the utmost level is equally important as understanding your adversary. When you understand who they are, your team will have easier time proactively looking for intrusions via threat hunting using the Cyber Threat Intelligence on each group, thus thwarting them before they even gain foothold into your network.

The insiders are a big issue right now. 90% of insiders are usually men between age of 30 to 50 who feel they have not reached their goals in life and as much as the Kenyan economy is now, most of them will agree to work with these groups. Identifying insiders is vital, to your infrastructure's security.

Otherwise, let's enjoy the holidays, keep your SOCs open throughout, be on a high alert, keep monitoring and reporting, maim and destroy any attempt of penetration.

Happy holidays from OnNet,