IMPERIAL TIGER - OLD TECHNIQUES IN NEW CAMPAIGN

INFO SECURITY TIMES: THREAT REPORT (JANUARY 28TH)

The threat actor known as Imperial Tiger appears to be making a resurgence since their initial campaigns almost 2 years ago. However, the group appears to be taking targeting easier exploitable machines in comparison to their previous attacks. Threat researchers have dubbed this campaign as the Devil's Garden and have noted some of the characteristics of this new campaign.

In previous campaigns, Imperial Tiger attacks have historically leveraged sophisticated malware that utilized custom written tools that no researcher had previously seen. Previous attacks also targeted industrial control system networks, indicating a level of sophistication that pointed towards potential government state sponsorship. This time around, the Devil's Garden campaign goal appears to be to infect networks and assets with a variant of ransomware, which lessens the likelihood of nation state attribution. This trend appears to indicate that the group is attempting to find new ways to generate income for future attacks

In recent attacks, incident response teams from a few organizations have reported that their employees have received macro enabled documents and spreadsheets via email that initialize the attack. Lab analysis of the phishing attacks indicate that Imperial Tiger has been keen on gathering organizational information prior to attacks to launch extremely believable spear phishing attacks. Once the victim opens the file their malware initially downloads a secondary payload from a website owned by the group. The secondary payload then uses file system exploits to move laterally to other assets on the same network. As each asset on the network is compromised the ransomware encrypts user files on the victim machine before posting the ransom note to the victim's desktop. The threat group does appear to return to their sophisticated roots though by leveraging dynamic DNS entries and file names in each new victim network.

While this campaign is relatively new, expect this threat actor to continue wreaking havoc as more victim organizations are targeted.

iLabs_Threat_Research @ilabsthreat – Feb 18

In light of recent findings of dynamic process name generation of the latest #DevilsGarden campaign, we have begun aggregating IOCs for this threat actor. DM us for additional information on how to submit information

----

Maligned @maligned– Feb 15

#DevilsGarden is a clear demonstration that old file transfer protocol versions, like SMB, SSL, etc… need to disabled in a timely manner…. Its 2020 for crying out loud

----

Joes_Bargain_Security @joebesec – Feb 16

Spent the last 3 days cleaning up a mess of machines infected by the #DevilsGarden ransomware variant. Noted that the machines all displayed connections back to various 94.x.x.x addresses, but had different file names for the malware. Trying to make sense of it.

----

iLabs_Threat_Research @ilabsthreat – Feb 18

In light of recent findings of dynamic process name generation of the latest #DevilsGarden campaign, we have begun aggregating IOCs for this threat actor. DM us for additional information on how to submit information

----

Defensive_Karim @Def_Karim – Feb 19

First rule vulnerability assessment is knowing what you have. Survey of your assets tell you where your vulns lie. #DevilsGarden

Hacker in the Attic

ANALYSIS OF IMPERIAL TIGER ACTIVITIES

(Feb 20th, 2020)

It has been most interesting if you are following the recent news regarding activity around Imperial Tiger campaign named Devil's Garden. One of the more interesting parts of this campaign is that it deviates from the norm of their previous activity, which largely targeted industrial control systems and critical infrastructure. However… here we are, faced with an increasing pandemic of ransomware attributed to this very same group. While the focus has shifted away from critical infrastructure as a specific target, the wormable ransomware variant in this campaign has proved to be ever painful for many organizations. From this, I've found some specific findings that I would like to outline in this quick and hopefully useful blog post.

First, the threat actor still retains very good open source intelligence capability. This allows them to tailor their spear phishing campaigns to organizations in a way that is not seen often in other campaigns

Second is the method used to compromise machines and having and initial loader download a secondary payload, the malware that performs encryption, lateral movement and the communicates with a C2 server

Third, the malware download appears to be leveraging one of many different file names for defense evasion while utilizing native PowerShell on Microsoft Windows machines. But, the threat actor did not do much in the way of utilizing a diverse range of IP address endpoints for C2 communications.

Finally, it was noted in a few cases that the initial dropper executed on the victim machine, but due to effective application whitelisting techniques stopped the malware from executing and encrypting some victim machines. Therefore allowing defenders to analyze running processes, memory dumps and file changes to learn more about the malware and adjust defenses appropriately.