Serianu Cyber Security Advisory

Fake Microsoft Teams Updates Lead to Cobalt Strike Deployment

Serianu SOC Advisory Number:

TA – 2020/023

Date(s) issued:

1st December, 2020

System Affected:

- Microsoft Teams

Overview:

The ongoing COVID-19 pandemic has forced a number of organisations and businesses to work from home. Many organizations are shifting to video conferencing solutions and threat actors are now taking advantage to exploiting the situation on remote workers. Over the course of this year, there has been a significant rise in the number of malware attacks.

Based on our research, attackers are using malicious fake adverts for Microsoft Teams updates to infect systems with backdoors, which use Cobalt Strike to compromise company's networks with malware. In addition to the attack vector mentioned above, the attack is targeting organisations in various industries but recent ones focused on the education sector (K-12), which depends on videoconferencing solutions and apps like Teams which depends on remote environment due to COVID-19.

Serianu is issuing this advisory, to update organisations about these Fake Updates campaigns and offering recommendations that would lower the impact of the attack and avoid falling into such traps.

Description

Malicious attackers are compromising search engine results to place their malicious ads at the top, which claims to be the latest update for Microsoft Teams. When a victim clicks on the link, they are redirected to a site that is controlled by the hackers i.e. it downloads a payload that executes a PowerShell script, which loads malicious content.

Unsuspecting users falling into this trap and downloading the fake update will end up having a backdoor in their systems, set by hackers. Besides executing a PowerShell script, hackers set up Microsoft Teams software on the victim's machine to avoid any suspicion. The backdoors are then used to invite payloads like Predator, an information stealer that retrieves sensitive data like credentials, browser and payment data from victim's machine and sent to the hacker's C2 (Command-and-control servers), these are used by attackers to maintain communications with compromised systems within a target network.

The next stage includes downloading Cobalt Strike beacons, which is a legitimate penetration testing tool often exploited by hackers for finding ways and moving across the compromised network.

Commodity Attack-Simulation Tool

Cobalt Strike is a commodity attack-simulation tool that's used by attackers to spread malware, particularly ransomware. Recently, threat actors were seen using Cobalt Strike in attacks exploiting Zerologon, a privilege-elevation flaw that allows attackers to access a domain controller and completely compromise all Active Directory identity services.

Cobalt Strike beacons are among the payloads also being distributed by the campaign, which gives threat actors the capability to move laterally across a network beyond the initial system of infection.

Recommendations

In order to prevent malware attacks, Serianu recommends users to:

1. Use web browsers that can filter and block malicious websites.
2. Use strong complex passwords for local administrators which cannot be easily guessed.
3. **Limit the admin privileges to essential users**: Service accounts with similar same permissions as an administrator should also be avoided to prevent domain-wide access.
4. **Block executable files that do not meet specific criteria**: This can be easily done by installing anti-spyware or anti-virus software that scan files and automatically remove malware and files that do not meet set criteria to limit the extent of the attacks.
5. Make sure all security tools are updated and detected malware is removed immediately.
6. Block JavaScript and VBScript code from downloading executable content.

Conclusion

Security remains an ongoing and never-ending task and it needs to be a high priority. Organisations need to protect themselves from malicious cyber-attacks.

Information Sharing

As a means of preventing such attacks from occurring, we encourage any organization or individual that has access to commonly related malware attacks to share it with us through our email info@serianu.com to allow us to analyze any indicators of compromise (IOC).