Uncovering Domains Created by Octo2's Domain Generation Algorithm

domaintools.com/resources/blog/uncovering-octo2-domains/

October 10, 2024

Introduction: What is Octo2?

Octo2 is a new version of one of the most prolific malware families, Octo (ExobotCompact). The banking trojan targets Android mobile devices and the newest version is likely to be seen globally in the coming year. The "Architect" of Octo released Octo2 after the original's source code was leaked earlier this year. The new version offers differentiating features including increased Remote Access Trojan (RAT) stability, improved anti-analysis and anti-detection techniques, and the use of a domain generation algorithm (DGA) to generate the actual C2 server name.

Researchers at DomainTools are particularly intrigued by the obfuscation technique involving the use of a DGA to generate the Command and Control (C2) server name considering our unique dataset of domains. Thanks to initial efforts by Infoblox's threat intelligence team, we were able to leverage our database and tools to quickly uncover additional domains matching Octo2's DGA pattern, which are shared in this blog.

Summary of Research Findings

Based on this article by Threat Fabric, the initial samples of Octo2 discovered in the wild were seen in Italy, Poland, Moldova, and Hungary. Researchers believe use may quickly spread considering the global adoption of the original Octo, improvements made in Octo2, and the creator listing the new version at the same price as the original.

In the first samples, the banking trojan has been seen to disguise itself as apps including Google Chrome, NordVPN, and "Enterprise Europe Network." Discovered attacks utilized a malware dropper called Zombinder, which activates upon downloading the fake app and prompts the user to install a plugin, which is actually Octo2. Once infected, Octo2 allows for remote access of the mobile device to intercept push notifications, harvest credentials with fake login pages, and perform unauthorized actions.

Octo2's use of a DGA to dynamically change its C2 server address makes it harder for security systems to detect and block. Using a DGA for the C2 server address is like being able to change the address of your evil headquarters on the fly. However, once researchers and other experts identify the pattern used to generate the domains for the address, it becomes easier to monitor any changes.

Looking for Domains Created by Octo2

The post from Infoblox's threat intelligence researchers lists several domains thought to be connected to Octo2. The original domains exhibited a DGA pattern, where the apex-level domains generated consist of a random string of 32 alphanumeric characters, paired with a top-level domain (TLD) selected from a specific set of options.

Using Iris Investigate, we were able to pivot off of the original domains' IPs to find additional domains matching the pattern. We were eventually able to expand the original 9 domains and 7 TLDs to 269 domains and 12 TLDs first seen from August 22nd, 2024 to October 4th, 2024.

It was encouraging to find that some domains in this group were already being sinkholed by other researchers and security groups. Sinkholing domains enables researchers to disrupt the malware's communication with its C2 server and gather valuable data on its behavior, infection rates, and geographic distribution.

Identifying DGA domains in the wild can also be achieved by analyzing traffic in a SIEM. Once discovered, obtaining additional context is crucial for risk-based decision-making. Iris Enrich (another subtle plug incoming) is an API designed to provide this contextual data, offering key registration and infrastructure information along with a predictive domain risk score to enhance decision-making.

Implications of Using Domain Generation Algorithms

With the rise of Malware-as-a-Service (MaaS), malware creators understand the importance of differentiating themselves from competitors. Utilizing a DGA as an additional layer of obfuscation has become a key evasion tactic employed by many groups.

One of the earliest and most notable examples of utilizing a DGA is the Conficker worm, which emerged in 2008 and was covered by our very own Joe St Sauver. In an effort to gauge current adoption levels, I stumbled across an article by Sigmund Brandstaetter who notes: “the threat landscape is extensive with well over 50 malware families known to utilize DGA domains.” Zeus and Dyre are malware families targeting financial information and banking details, to name a few.

In the SolarWinds attack, SUNBURST malware used a DGA to generate domains encoding compromised computers. These domains resolved to IP addresses to assess value, then either connected to a C2 server, continued beaconing, activated a kill-switch, or switched to passive mode based on the subnet. Once the DGA was identified, Farsight used its real-time DNS resolution observability to detect beaconing activity from likely compromised environments. This data was publicly released and used by defenders and investigators, such as Bambenek Consulting’s indicator repository. For a deeper dive, check out this post-attack analysis on how passive DNS data pairs well with Maltego.

As DGAs become increasingly common among malware families, there is a heightened emphasis on the importance of domain-related data. Once researchers and security practitioners are able to detect malware using DGAs, being able to pivot and expand on associated domains allows for a better understanding of the pattern utilized. Rapidly identifying the DGA pattern significantly shortens the time from detection to mitigation, thereby reducing the success rate of malicious activities and enhancing overall internet security.

Practical Advice to Avoid Octo2 Infections

If you are a security practitioner looking to avoid Octo2 infections, here is some practical advice.

1. Leverage Threat Intelligence and Domain-Related Data:
    1. Utilize threat intelligence feeds such as known malicious DGA lists to stay updated on the latest Indicators of Compromise (IOCs) related to Octo2.
    2. Perform contextual data analysis and expand on known associated domains to detect patterns quickly and mitigate accordingly.

2. Implement Advanced Detection Tools:
    1. Use advanced malware detection tools that can identify unusual patterns in network traffic. Tools like sandboxing and machine learning-based anomaly detection can be particularly effective.
    2. At DomainTools we offer a suite of data feeds such as those deemed to be the riskiest, newly active, or youngest to help with malicious domain detection.
3. Monitor DNS Traffic:
    1. Regularly monitor DNS traffic for suspicious domain queries. DGA domains often have unusual characteristics, such as random-looking strings or frequent changes.
    2. Consider using protective DNS tools to perform content filtering and block malicious domains at the DNS security layer.
    3. Investigating suspicious domains within DomainTools passive DNS database can help establish timelines and find connected infrastructure.
4. Deploy Endpoint Detection and Response (EDR):
    1. Implement EDR solutions to monitor and analyze endpoint activities. These tools can help detect malicious behaviors associated with Octo2, such as unauthorized remote access or unusual application behavior.
5. Collaborate with the Community:
    1. Through active engagement with the cybersecurity community to exchange insights and strategies for threat detection and mitigation, we discovered Octo2 and its new features. People helping people is powerful stuff.
    2. You can connect with us on X, Mastodon, or on CTI Grapevine.

Conclusion

The emergence of Octo2 underscores the evolving sophistication of malware and the critical need for advanced detection and mitigation strategies. By leveraging domain-related data and collaborating with the cybersecurity community, we can stay ahead of threats like Octo2. The use of DGAs by malware authors presents a significant challenge, but with the right tools and intelligence, we can better disrupt these malicious activities.

The collective effort of the cybersecurity community is essential in this fight. Sharing insights, strategies, and data not only helps in identifying and mitigating threats more efficiently but also strengthens the overall security posture of the internet. Together, we can create a safer digital environment for everyone.

A special thank you to Michael Klatt and Sean McNee for digging into this one as well. Most investigations are a group effort and we have a great group here at DomainTools.

Find domains and IOCs on our GitHub

Finding Octo2 Domains using DomainTools Iris Investigate – Watch on YouTube

Utilizing Passive DNS for Octo2 Investigation – Watch on YouTube