DAMBALLA

Peer-2-Peer: A Growing Tactic Used for Threat Command & Control

Damballa – 2013

Summary

Threat operators and malware authors have a long history of staying one step ahead of the security industry with their evasion tactics. As threat actors vary their techniques and methods and take a dynamic approach to skirting detection, the security industry is challenged to react to constantly changing offensive threats.

Similar to how malware authors can systematically and programmatically construct and armor thousands of variants of unique malware[1] binaries to avoid signature matching, today's threats have also adopted different approaches to hide the command-and-control facets of their threat communication.

Peer-2-peer (P2P) communications is one of the tactics gaining popularity among threat operators and bot masters for obscuring command-and-control communications. By using a decentralized communications paradigm of infected "peers" serving as server and host, the threat operators now have an "indestructible" communication structure that cannot be easily discovered from dynamic malware detonation or severed by the takedown of command-and-control servers. What was seen as a weak link, the centralized command structure of infected assets communicating to command-and-control servers, has now been taken away.

For the security industry and enterprise security teams, this means another shift in detection targets. Simply detecting static command-and-control addresses or call-back information from blacklists such as Zeustracker will not be enough to discover threats in a network and will increase the gap between evasion and detection.

In this brief, Damballa look at a sampling of a few recent threats that have P2P capabilities.

1. **ZeroAccess**
2. **Zeus V3/Gameover**
3. **TDL4/TDSS**

Peer-2-peer (P2P) communications is one of the tactics gaining popularity among threat operators and bot masters for obscuring C&C communications. By using a decentralized communications paradigm of infected "peers" serving as server and host, the threat operators now have an "indestructible" communication structure that cannot be easily discovered.

A Sample of Current Threats Using Peer-2-Peer

- ## ZeroAccess

  The operators behind ZeroAccess use a rootkit-based threat that primarily carries out click fraud and BitCoin mining. This threat uses various exploit kits, including Blackhole, Neosploit, and Sweet Orange, to spread itself. It also uses pay-per-install affiliates for infection campaigns. ZeroAccess downloads Trojan-laden applications that conduct web searches and click on results to make money through pay-per-click advertising. This malware's main form of communication is P2P.

P2P

Alternative Names:	ZeroAccess,ZAccess,W32/Trojan.Zeroaccess ZeroAccess.BX/ZeroAccess, Sirefef	Global Severity:	High
Threat Type:	Information Stealer (Information Theft & Sublease tool)	Antivirus Coverage:	Minimal

Threat behaviors: Rootkit and Trojan (Rootkit that downloads additional threats)

The primary motivation of this threat is to make money through pay-per-click advertising of criminally staged advertisements. An obfuscated application is downloaded, conducts Web searches, and clicks on the results. This technique is called click fraud, and it is a very lucrative business for malware creators because they avoid having to commit numerous illegal banking transactions from traditional bot infections. This technique became mainstream for malware authors in late 2010 because it decreases the risk to the criminal by avoiding crimes like identity theft and financial fraud that are more likely to be prosecuted.

ZeroAccess is also capable of downloading other threats onto the compromised computer. These threats may be misleading applications that display false information about threats found on the computer and scare the user into purchasing fake antivirus software. It is also capable of downloading updates of itself to improve and/or fix functionality of the malware. Furthermore, it may open a back door and connect to a C&C server, which gives the remote attacker access to the compromised computer. The attacker is then able to perform any number of actions on the computer, and the computer may then become part of a wider botnet.

The above functions are accomplished covertly as it infects a system driver that acts as a rootkit hiding all of its components on the system. The threat creates an encrypted obfuscated volume on the victim's file system, where it stores all of its components and hides any other malicious software that it downloads onto the computer.

- ## Zeus V3 - Gameover

The operators behind the Zeus V3 threat use a variant of Zeus, a banking Trojan that steals sensitive financial data, provides remote access capabilities to the infected system, and disables host-based security measures such as firewalls. This threat has been known to use the Cutwail spam botnet for initial malware distribution. This Zeus variant is typically first downloaded via the Pony loader malware and then includes the ability to use P2P protocol for C&C communication. If the hard-coded peers in the Zeus binaries cannot be reached, it falls back to a domain generation algorithm (DGA) seeded by the current date. The DGA produces 1,000 pseudorandom domains per day.

P2P/DGA

Alternative Names:	Zeus -V3 GameOver	Global Severity:	High
Threat Type:	Trojan (Multipurpose)	Antivirus Coverage:	Minimal

Threat behaviors: Trojan (steals sensitive financial data downloads additional threats)

Zeus V3 has a diverse set of features to capture information from a victim through keystroke logging, form grabbing, and credential scraping. Multi-purpose threats may also open a system to other threat downloads, making it vulnerable to other types of attacks.

- **TDL4/TDSS**

  The TDL/TDSS Gang (aka Tyler Durden Loader) operator uses malware in the form of a Master Boot Record (MBR) infector, targeting Microsoft Windows systems. The TDL rootkit utilizes MBR hooking, a process that deceives a user by appearing to be "initially deleted." Upon a system restart, the rootkit/Trojan is re-installed. This provides the remote attacker highly persistent backdoors into victim systems. To receive C&C instructions, TDL4 includes advanced communications techniques such as DGAs and P2P, which serve as either a primary or fallback mechanism if direct C&C communications are blocked.

  DGA/P2P

Alternative Names:	W32.Rootkit /W32.Alureon/ W32.Renos/W32.TDSS/W32.DNSChanger	Global Severity:	Critical
Threat Type:	Information Stealer (Information Theft & Sublease tool)	Antivirus Coverage:	Partial

Threat behaviors: Downloads rootkits and steals sensitive information

The TDL/TDSS rootkit has been observed spreading via spam and phishing e-mails. The observed stages of infection are as follows:

1. Infect a victim (Stage 1) via spam, drive-by-downloads, and malicious attachments.
2. Wait idle until the Stage 2 Trojan is ready for download.
3. Load a rootkit Trojan (Stage 2).
4. Alter the system to obfuscate Stage 1 and 2 infections (Stage 3).
5. Infect other sites, allowing third-party access to sensitive information.

Capabilities:

After an initial infection, the Stage 2 rootkit is normally loaded via a fast-flux worm. Once the infection has passed to Stage 3, various other threats (such as ZeusBot, Buzus, RogueAV, PoisonIvy, etc.) may be installed and utilized by threat operators. The authors behind TDL/TDSS are members of a professional criminal organization that also offers affiliate funding to anonymous distribution providers, infection operators, and other criminals.

About Damballa

As the experts in advanced threat protection, Damballa discovers active threats that bypass all security prevention layers. Damballa identifies evidence of malicious network traffic in real time, rapidly pinpointing the compromised devices that represent the highest risk. Our patent-pending solutions automatically detect and terminate criminal activity, stopping data theft, minimizing business disruption, and reducing the time to response and remediation. Damballa protects any device or OS including PCs, Macs, Unix, iOS, Android, and embedded systems. Damballa protects more than 300 million endpoints globally at enterprises in every major market and for the world's largest ISP and telecommunications providers.

For more information, visit http://www.damballa.com, or follow us on Twitter @DamballaInc

[1] https://www.damballa.com/downloads/r_pubs/WP_SerialVariantEvasionTactics