McAfee Labs

A Dummies Guide to 'Insider Trading' via Botnet

By Raj Samani on Nov 20, 2015

This post, the first of two parts, was written by Raj Samani, Christiaan Beek, and Shane Shook.

Want to spread malware? One of the most effective ways is to use a botnet, a network of infected systems. The goals of botnets have barely changed since we first encountered them more than a decade ago. We have often said that fighting cybercrime is a game of cat and mouse, with innovation from each side tipping the balance first one way, and then another. The evolution of botnets is no different.

In addition to common botnets plaguing our home computers to deliver spam or worse, we also find botnets targeting corporations to surreptitiously extract large collections of data to support incredibly profitable campaigns. These campaigns are aided by stolen credentials and the live viewing of (or interaction with) victims' systems containing confidential information. These steps allow an attacker to get an insider's view of infected organizations without actually being an insider —all while remaining undetected and manipulating data for financial gain.

In this two-part series we will first examine the evolution of the botnet, and follow up with a second post that shows how this new operating model is being actively used.

Botnet evolution

Originally robot networks were designed and used to enlist as many nodes as possible in criminal campaigns.

Traditional botnets focused on intrusion and data theft to perform the following activities:

- Remote control of systems.
- Interruption/denial of service.
- Personal information theft (identity/personal credit/banking).

Over time, botnets began to incorporate other services:

- “Doxing”/cataloging/selling stolen information.
- On-demand targeting and access provisioning to corporate systems.
- Third-party malware installation (RATs or ransomware) on systems.

Today, botnets provide managed services that include:

- Anonymous communications routing and publishing.
- Access management to subscribed networks/computers.
- Help desk services: including 24/7 technical support.
- Payment services (for electronic funds transfers or “crypto” currencies transactions).
- Markets for “dark web” products and services.

The actors behind these botnets, the “botmasters,” use these operations to serve a bigger collective of campaigns by renting access to others, as well as for personal gain.

Intel Security recently published the *McAfee Labs 2016 Threats Predictions,* which included a five-year forecast of the cybersecurity marketplace and its actors. In that article we mention that we do not quite expect the transformation of cybercrime into a full-fledged industry with suppliers, markets, service providers (“cybercrime as a service”), financing, trading systems, and a proliferation of associated business models.

However, this transformation, better described as an evolution, has been a product primarily of botnets, in which the botmasters now allow subscribers to request, view, and use protected and sensitive information. As customer needs and desires change, botnet services evolve to meet the demand.

Payment for these services are often made with Bitcoins.

Traditional botnets were “owner operated,” but as their financial success and reputation grew, they became organized. The evolution of botnets from botmasters defining services to subscribers demanding products and services, has led to a customer-oriented industry. Subscribers vary, but their interests are generally reflected by the malware types in modern botnets that include:

- Personal information stealers are targeted at consumers, most often through spam or phishing, and seek credentials and other personally identifiable information that facilitates identity and personal financial credit, banking, and trading theft.
- Corporate information stealers are targeted at corporate employees or officers, commonly through phishing but also supported by social engineering techniques to target individuals or business functions that can facilitate the theft of human resources information, or credentials (and computer access) for financial (ERP/ACH/EFT) fraud and theft.
- Market information stealers are delivered via targeted phishing, or they use sophisticated marketing techniques such as “waterholing,” by infecting advertisements served to websites frequented by particular industry readers, or business networking services that create trusted links between people upon request or via introductions through social media. These are usually targeted at corporate officers of public companies, lawyers or auditors, or employees of financial services institutions and related media services. Information stealers facilitate the theft of protected or sensitive market information that can be used for insider trading.

The malware used are common in their design, differing only in whom they target, which instructions they employ to harvest different types of information, and which control sites they communicate with. Defining the type of crime is no longer about the tool(s) being used, but the evidence of activity. This evidence exists fundamentally in only three places: the control servers where stolen information is stored and made accessible to subscribers, victims’ financial (or trading) accounts where fraud has been conducted, and victims’ computer artifacts where the history of misuse can be assessed.

Let’s look at some examples.

Personal information stealer: This tool injects malware into browser processes to collect credentials used to conduct financial or securities transactions with the consumer's bank. Modern malware types such as Dyre leverage additional features including remote desktop "back connects" that also allow botnet operators or subscribers to use the infected computer to log on to the consumer's bank sites. Today's information stealers even incorporate tools to defeat two-factor authentication through screen shots or other techniques.

Corporate information stealer: This method not only harvests credentials in a similar (though expanded) method as with personal information stealers, but the malware also facilitates backdoor access to the corporate network. The malware automatically collects system information about the compromised computer, user credentials and permissions, and —according to other scripted instructions—accessible corporate network information. The botmasters then catalog that information and either conduct additional reconnaissance and exploitation of the compromised corporate computer or network, often installing additional RATs to create multiple and persistent access to the organization, or simply sell th[illegible] that they have access to certain computers in certain [illegible]ate estates to willing subscribers. Those subscribers subsequently either direct additional activities if the botmaster provides those services, or use the access for their own purposes.

Watch for part two of this post.

Contributors

We would like to thank the many people involved in this research, including members of the Malware Operations team, the Malware Sample Database team, the Foundstone Incident Response team, and our special coauthor of this research, Dr. Shane Shook.

Dr. Shook is well-known to Fortune 100 global companies for providing experienced leadership in incident analysis and response. He has led small and large teams of forensic investigators and computer and telecommunications systems analysts in many of the most notorious information security breach events of the past two decades. Shook's experience in financial services and other industries, including standards development, helps Intel Security clients understand

technology risks in the context of their businesses.

Tags: botnet, computer security, cybercrime, malware, network security, Quarterly Threats Report

No Comments

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Comment

Type the text

Privacy & Terms

Post Comment