IT Security House

ITSH Paper – April 2016

Tracking Cyber Crime Campaigns

Author - Stefan Frei, Ph.D.

Abstract

Cyber criminals effectively exploit the opportunities provided by the rise of the Internet and have, in just a few years, successfully stolen hundreds of millions of dollars from organizations of all kinds across the globe. The capability of cyber criminals to centrally control millions of compromised victims, by the use of botnets, allows them to effectively and quickly adapt and launch new and targeted campaigns. As prevention is limited, organizations are faced with the dilemma that they have to do business with a considerable share of infected clients, that in turn call for new approaches to combat these threats. ITSH is powered by CSIS Security Group A/S[1] vast network of sensors and sinkholes to track botnet activity and cyber crime operations by analyzing the source: *the bots and their control servers*. The continuous collection and analysis of this data provides formidable insight into cyber crime campaigns and tactics as well as timely information on the organizations being targeted.

This paper explains how cyber criminals are able to operate botnets that compromise victims on a large scale, and informs organizations about how to best utilize cyber threat intelligence to protect their business and deal with infected customers.

In today's threat environment, security is as much about remediation as it is about prevention.

[1] CSIS Security Group A / S – www.csis.dk

Table of Contents

1. Introduction

An advanced malware attack can no longer be seen as a single incident consisting of exploit, infection, and remediation stages. Today's attacks are well-coordinated efforts to infiltrate an organization, or a large number of private users, and establish a foothold for the purposes of reconnaissance, exploitation, data exfiltration, and ongoing surveillance.

Botnet Infrastructure

The primary infrastructure of cyber criminals to execute such campaigns are botnets – a massive network comprised of compromised machines ("bots") and command & control servers ("C&C") to control the botnet, as shown in Figure 1. A bot depicts any compromised machine in corporate or private use. C&C servers are a key component of botnets allowing cyber criminal to effectively control millions of bots. C&C functionality is typically installed on compromised machines, in order to obfuscate the identity of the bot master(s).
The bigger a botnet, the more it can do because of its members' compounded bandwidth and computing power. Besides hijacking user sessions, parts of a botnet can easily be rented out to other gangs or re-tasked for distributed denial of service attacks ("DDoS"), spamming campaigns, distributed bitcoin mining, or password cracking.

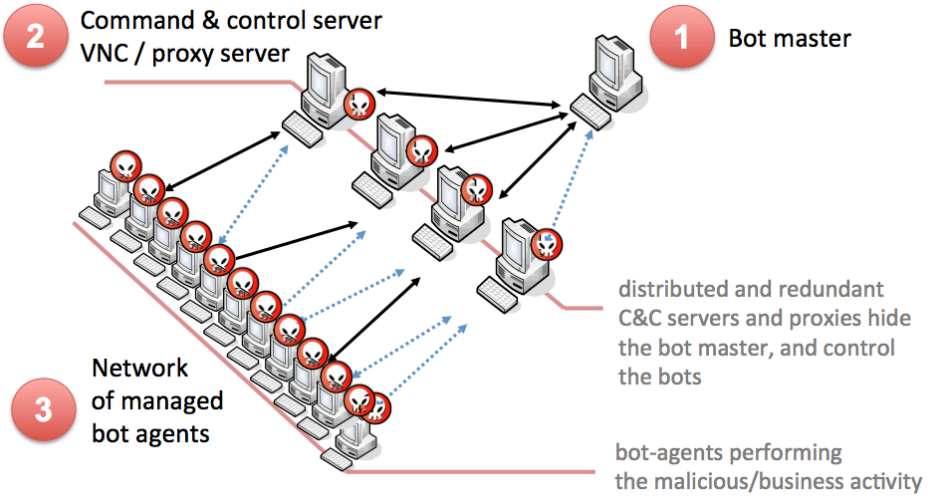

Figure 1 – Components of a botnet

Bot Master

The bot master controls the network of compromised PCs through intermediate layers of C&C servers. These layers of C&C servers effectively shield the controlling bot master from identification, and provide resiliency against individually failing C&C servers.

Command & Control ("C&C")

A distributed and redundant set of compromised machines acting as management servers. New instructions, payloads, and configurations prepared by the bot master are distributed to the bots through the C&C servers. Key functions of a C&C server:

- Administrative and management panel for the bot master
- Push updates to bots
- Repository of data harvested by the bots
- Act as proxy between bot and bot master

Bot

A software agent on the compromised victim machine. The bot permits remote control of the victim machine by a C&C server, and executes the malicious activities: key stroke logging, disabling anti-malware programs, and information harvesting. The bot always runs in the background and activates specific functionality to hijack sessions and credentials whenever the user visits a targeted web site (*web injects*, defined later).

The continued and active control of botnets allows cyber criminals to push new campaigns and targets to millions of compromised machines – and to act swiftly to render countermeasures ineffective. Cyber criminals can further re-task a bot by simply pushing an updated configuration onto the C&C servers, which will distribute the new information to all connected bots. This includes the download and execution of new exploits as well as execution commands and capabilities.

To build botnets, cyber criminals have to first compromise a large number of victims, and then establish a secure and robust communication channel in order to control the victims.

2. Botnet Buildup

Attack Vectors

In order to compromise a large number of victims cyber criminals either deploy exploit kits that poison search results, infect web advertisements, or otherwise redirect users to the exploit kit. The main techniques used to infect web sites and subsequently compromise workstations are "spear phishing" and "software exploitation":

Spear Phishing	In a spear phishing campaign, cyber criminals use public sources such as *LinkedIn, Xing, Facebook*, or a *company web site* to gather information on likely targets. Using this information they send credible e-mails to the victims that purport to be from a trusted source, but actually contain droppers that install malware.
Software Exploitation	Once the user is redirected to the exploit kit, the user's machine gets infected and the bot is installed. Typically, cyber criminals do not need 0-day attacks[2]. A large number of systems worldwide still run the outdated versions of the operating system, the web browser, or many of the programs installed are not on the latest patch level.[3]

Figure 2 – Main attack vectors to compromise end-points

Evasion of Detection

To bypass malware detection engines, cyber criminals automatically generate tens of thousands of unique permutations of the original malware while retaining the core functionality of the malware. Thereafter each target is attacked with a unique sample of the malware – which makes detection of malware a tedious task. Cyber criminals further ensure their attacks go undetected by prior testing of malware samples against all anti-malware solutions on the market. Only samples not detected in these tests are then used for attack campaigns. This method continually proves to be very effective at bypassing malware detection engines, and compromising systems at large scale.

Post Infection Activities

After successful infection of the target, the bot connects to the C&C server to upload the full information of the user and the specification of the infected machine. It then downloads and installs specific payloads and configuration information prepared by the cyber criminals for the new target. This includes rules and functionality to disable locally installed anti-malware programs, and prevent the machine from accessing or getting updates from security sites. The malware lies dormant until the user visits a web site specified in the bot configuration file – which then activates the attack and the hijacking of the user session, amongst other malicious activities.

[2] The Known Unknowns in Cyber Security - http://techzoom.net/Publications/Papers/knownunknowns
[3] Flexera Country Report US 2015/Q4 - http://media.flexerasoftware.com/documents/Research-SVM-US-2015Q4.pdf

Thus, malware is designed to operate invisibly, making the identification and remediation of compromised systems an expensive endeavor – and results in extended times of compromise.

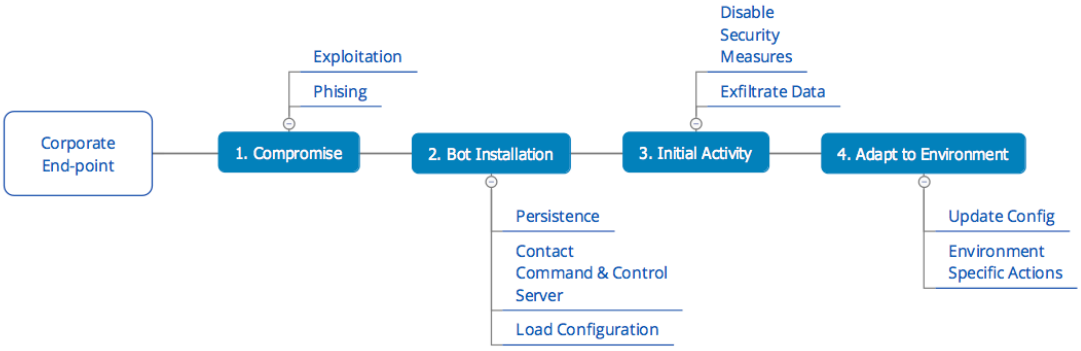

Figure 3 – Typical post-infection activities and live cycle of a bot

3. Controlling the Botnet

Cyber criminals go to great length to secure their control over the botnet against takedown attempts from law enforcement, the security community, or competing cyber crime gangs. To operate the botnet, the bot master has to address the following challenges:

A. Anti-malware engines and security updates on the infected machine might disable and remove the bot.
B. The communication between the bot and the C&C servers might be disabled or taken over by a third party resulting in the bot master loosing control over his botnet. Or, in some cases, the new malware will remove the existing malware and the compromised host will become part of a new botnet.

The former challenge is a lesser issue for criminals as this approach implies to take action against the botnet on millions of globally distributed machines – a daunting task which does not scale well. Further, upon initial compromise of a machine, the bot disables anti-malware functionality or renders it ineffective.

Securing the C&C infrastructure and communication channel of the botnet represents the true challenge to cyber criminals. To control millions of bots in a robust manner cyber criminals operate an array of globally distributed C&C servers - hosted themselves on infected machines – to which the bots connect. A robust method to allow a bot to identify a suitable C&C server, and switch to another C&C server if one is found unresponsive, was therefore developed by criminals.

3.1. Domain Generation Algorithm ("DGA")

It is evident that bots cannot rely upon a static list of preconfigured domain names or IP addresses that correspond to existing and future C&C servers, as these are easy to identify and blacklist. Instead, cyber criminals have designed domain generation algorithms ("DGA") that given a particular date, time, and seed value will produce a large number of seemingly random candidate domains.[4] The bot will then cycle through this list until it finds a "live" C&C server. The bot master, knowing the sequence of domains generated, only needs to register a few of these domain names to ensure control over the botnet.

The purpose of a domain generation algorithm is to:

- Make it impossible for static reputation systems to maintain an accurate list of all possible C&C domains.
- Maintain a small but agile physical C&C infrastructure that only needs to be configured and turned on for short periods of time.
- Provide the bot master "just-in-time" registration of domain names to avoid reactive counter-measures employed by law enforcement.

The large number of potential rendezvous points (thousands of domain names generated per day) makes it difficult for law enforcement to effectively shut down botnets since infected computers will attempt to contact only some of these domain names every day to receive updates or commands.
Further, all communication with the C&C servers is typically encrypted and signed, to prevent unauthorized parties from hijacking the botnet after decoding the communication protocol in use.

4. Threat Intelligence on Botnets

Botnets are very interesting, albeit difficult to fully analyze. A formidable approach to gather live intelligence on ongoing botnet operations is sinkholing:

Sinkholing

Sinkholing is a technique that is used to redirect the traffic from bots to an analysis server. To identify and connect to the botnet's C&C servers, malware typically uses either hardcoded fail-over domains or a DGA to generate possible rendez-vous points with one of the C&C servers. Reverse engineering of infected machines allows security researchers to identify and buy/register some of the rende-vous domains, and thereby

[4] DGAs in the Hands of Cyber Criminals - https://www.damballa.com/downloads/r_pubs/WP_DGAs-in-the-Hands-of-Cyber-Criminals.pdf

redirect all traffic of infected bots to the sinkhole server where intelligence is collected and analyzed once a bot uses one of these domains.

Identification of Compromised Machines

Knowledge of the sequence of domain names generated by the DGA's can be further used to protect organizations, identify infected machines, and prevent the bot from communicating with the botnet or the exfiltration of data. For example, ITSH exposes the domain names generated by DGA's through their Secure DNS service offering based on sinkhole data of CSIS Security Group A/S.[5]
This service allows organizations to easily identify infected machines that attempt to contact the bots C&C server, and thereby:

- Effectively prevent internal machines from exfiltration of data as the bot can no longer connect to the C&C server.
- Allow public facing services such as web portals, mail servers, or e-commerce sites to identify compromised clients and adopt the security of the session accordingly.

Due to the knowledge gleaned by reverse engineered DGA's, the sequence of domain names for this service can be generated ahead of time, and thereby provide proactive protection.

Tracking of Cyber Crime Campaigns

Sinkholing also exposes the configuration files pushed by cyber criminals to the bots. These configuration files contain a wealth of timely and accurate information on ongoing cyber crime campaigns and the organizations targeted by these campaigns. The systematic analysis of botnet configurations enables the ability to track cyber crime campaigns at the very source. The two main sections of configurations files are *domain blacklists* and *webinjects*:

Domain Blacklists

In order to prevent the victim from automatically, or manually, updating the machine and any anti-malware solution, domain-blacklists contain an array of domains that the bot permanently blocks. Figure 4 shows the top 15 most frequent blacklist entries of the botnets tracked by the ITSH eCrime service data from 2016/Q1. These blacklists are very extensive (1k entries) and updated frequently to disable the widest range of security products.

[5] ITSH Secure DNS Service- http://itsechouse.com/products/sdn/index.html

Rank	Target Domain	Botnet Family	Frequency
1	mcafee.com	Citadel ZeuS Gameover	
2	trendmicro.com	Citadel	
3	avast.com	Citadel	
4	kaspersky-labs.com	Citadel	
5	microsoft.com	Citadel ZeuS Gameover Zeus	
6	f-secure.com	Citadel	
7	com.ua	Citadel	
8	bitdefender.com	Citadel	
9	avg.com	Citadel	
10	clamav.net	Citadel	
11	avira.com	Citadel	
12	comodo.com	Citadel	
13	symantec.com	Citadel	
14	grisoft.cz	Citadel	
15	nai.com	Citadel	

Figure 4 - Top 15 organizations/domain names blocked by bots to prevent security updates (2016/Q1 data from CSIS Security Group A/S)

Web Injects

A web inject is specific HTML code injected into the victims browser session in order to provide exfiltration of sensitive data, e.g. user name and password upon authentication, or to insert fraudulent transactions. Figure 5 shows a typical login page of a corporate web application together with the same page modified by a web inject with the goal of exfiltration of the original data and the now additional "ATM pin."

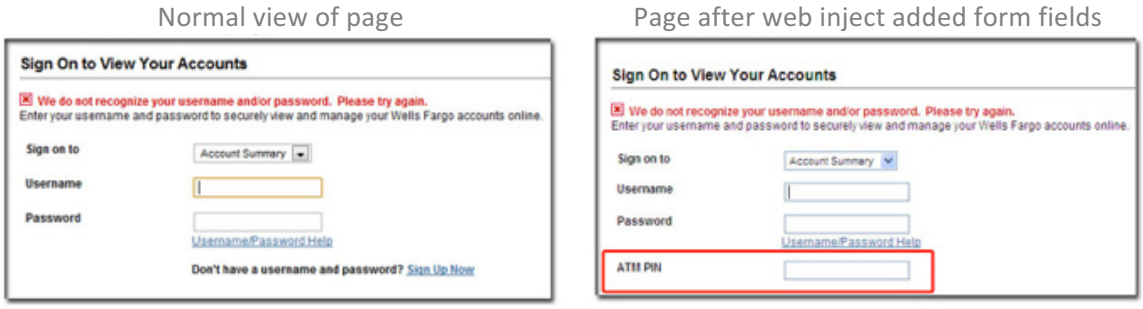

Figure 5 – Original view of an account login page (left); the page modified by web inject to exfiltrate the users username, password, and the ATM pin (right)

Web injects are tailored to the web sites targeted by criminals, and may change from campaign-to-campaign. Target lists contain the domain names/URLs together with the HTML/JavaScript code of the specific web inject. Figure 6 shows the top 15-targeted organizations/domains based on the ITSH eCrime service data from 2016/Q1[6]. The bot

[6] ITSC eCrime Service - http://itsechouse.com/products/ecrime/index.html

checks every web request of the victim against the target list. Only accessing a targeted web site (e.g. ebay.com) will activate a specific web inject.

Rank	Target Domain	Botnet Family	Frequency
1	bankofamerica.com	Citadel Cridex Ice9 Neverquest Zeus	
2	wellsfargo.com	Citadel Cridex Ice9 Neverquest Zeus	
3	tdbank.com	Citadel Cridex Neverquest Zeus	
4	discovercard.com	Citadel Neverquest Zeus	
5	paypal.com	Citadel Cridex Ice9 Neverquest Zeus	
6	53.com	Citadel Cridex Ice9 Neverquest Zeus	
7	citibank.com	Citadel Cridex Ice9 Neverquest Zeus	
8	halifax-online.co.uk	Citadel Cridex Gootkit Ice9 Neverquest Ramnit Tinba Zeus	
9	chase.com	Citadel Cridex Ice9 Neverquest Zeus	
10	yandex.ru	Citadel Ice9 Zeus	
11	americanexpress.com	Citadel Neverquest Zeus	
12	hsbc.co.uk	Citadel Cridex Gootkit Ice9 Neverquest Zeus	
13	pnc.com	Citadel Cridex Neverquest Zeus	
14	barclays.co.uk	Citadel Cridex Gootkit Ice9 Neverquest Ramnit Tinba Zeus	
15	com.my	Citadel Cridex	

Figure 6 – Top 15 organizations/domain names targeted by web injects in 2016/Q1 based on CSIS Security Group A/S data

The ITSH eCrime service is based on up-to-the-minute telemetry data on thousands of bot configuration files covering numerous active malware campaigns and botnet families. This data provides direct and formidable insight into the activities of cyber criminals, their capabilities, and current campaigns. Updates in bot configuration files are closely monitored and automatically compared against the domain names of customers for rapid alerting.

Domain	Botnet Family	Target URL
ebay.com	Citadel, Ice9, Zeus	*.ebay.com/*eBayISAPI.dll?*
my.ebay.ca	Citadel	*my.ebay.ca/ws/eBayISAPI.dll?MyEbay*
my.ebay.co.uk	Citadel	*my.ebay.co.uk/ws/eBayISAPI.dll?MyEbay*
my.ebay.com	Citadel, Ice9, Zeus	*/my.ebay.com/*CurrentPage=MyeBayPersonalInfo*
my.ebay.de	Citadel	*my.ebay.de/ws/eBayISAPI.dll?MyEbay*
my.ebay.fr	Citadel	*my.ebay.fr/ws/eBayISAPI.dll?MyEbay*
signin.ebay.*	Zeus	https://signin.ebay.*/ws/eBayISAPI.dll*
signin.ebay.com	Citadel	*signin.ebay.com/ws/eBayISAPI.dll?SignIn*

Figure 7 – Example web inject target list - targeting various specific parts of the eBay web portal based on sinkhole data from CSIS Security Group A/S

The full information of the web injects are extracted from the configuration files and are readily available for analysis and expedited development of countermeasures.

Conclusion

Over the last few years the industry has come to realize that full-protection, or prevention, of cyber threats is an illusion. Cyber criminals continuously prove their ability to circumvent any kind of new defense measures introduced, and to quickly identify the weakest link in the security chain.
Typically, organizations have implemented extensive backend protection and monitoring on their systems. These are normally paired with best practice controls from compliance frameworks. However, this still leaves the organization with the dilemma that it has to do business with a considerable share of infected clients (an infrastructure they do not control).
A thorough understanding and monitoring of cyber criminals capabilities is essential to prepare against, and defeat, modern attacks. Without viable threat intelligence on cyber crime operations, organizations focus on defending against known threats and will be taken by surprise by every new security challenge or breaches. Research shows this happens with unnerving frequency.

To address these challenges:

- Enterprises must be prepared to do business with a large number of already compromised clients.
- Enterprises should assume their network is already compromised, and assume that it will continue to be compromised.
- As prevention is limited, enterprises should deploy tools and processes to quickly detect and remediate successful breaches, and detect compromised customers connecting to their systems.
- Enterprises should respond to a breach with a well-defined process rather than considering it to be an exception; have in place an incident response plan that is subject to routine review.

Organizations should therefore investigate the benefits of collaborating with industry partners to enhance real time threat intelligence for their continued risk assessment and antifraud efforts – and ensure they can handle an internal compromise effectively.

In today's threat environment, security is as much about remediation as it is about prevention.

© 2016 – All rights reserved.
All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, or otherwise without the prior permission of IT Security House or the authors.