Malware: New Capabilities & Directions

An analysis of a modified *Carberp* botnet

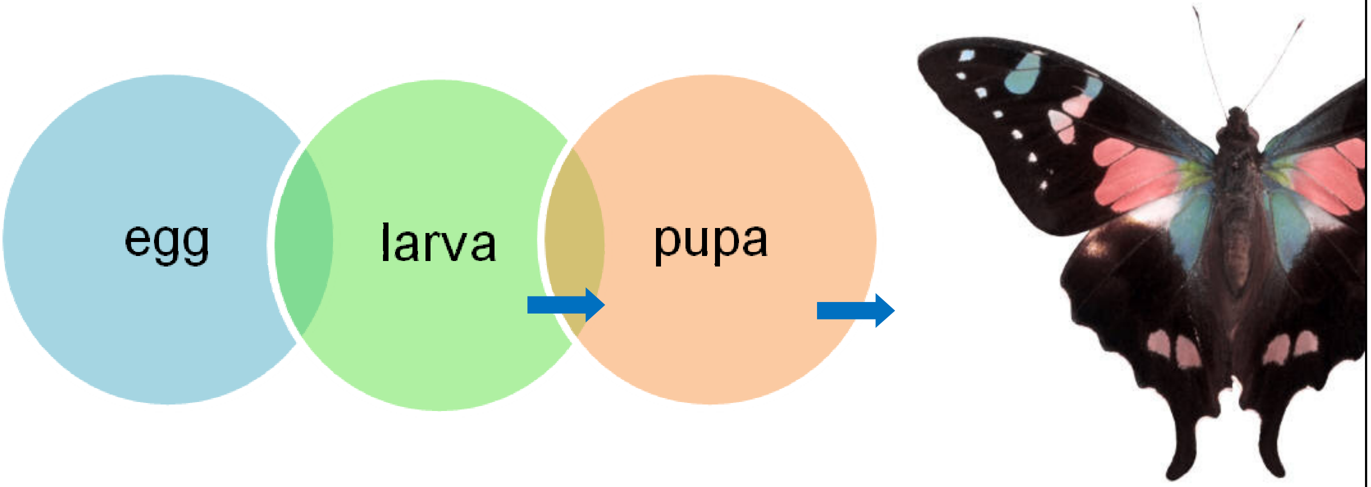
by

Jim McKenney, MBA, GPEN, GSNA, CISA, CISM

Jims67mustang@gmail.com

http://www.linkedin.com/in/jimmckenney

TABLE OF CONTENTS



1. INTRODUCTION

In late 2011 a forensics investigation led to the access of the *Command & Control* operations of a modified *Carberp* botnet composed of 603 computers. The computers were located in Kansas, Missouri, Oklahoma and Nebraska.

While this network is considerably smaller than those studied by antivirus and security vendors, the investigation still yielded interesting data and raised the possibility that considerable effort was being made to bring intelligence into asset tasking and ranking.

In order to verify that automated intelligence-driven decisions was being used by the Botnet administrators, a separate OLAP server was created to perform linkage and multidimensional analysis on the data collected by the *Carberp* botnet. The experiment was successful; replicating the asset tasking logic and assigned confidence values found on the Command and Control platform.

2.SUMMARY

The investigation validated current capabilities of the *Carberp* platform and provides insight into malware network development direction and focus.

2.1 VALIDATION OF CURRENT CARBERP CAPABILITIES

> *1. Disabling or crippling antivirus controls*
> *2. Universal credential harvesting*
> *3. Disabling security updates*

2.2 EVIDENCE OF NEW MALWARE CAPABILITIES

> *1. Use of rudimentary linkage analysis techniques to determine asset value*

2. Long-term compromises
3. Advanced Encryption & Obfuscation techniques

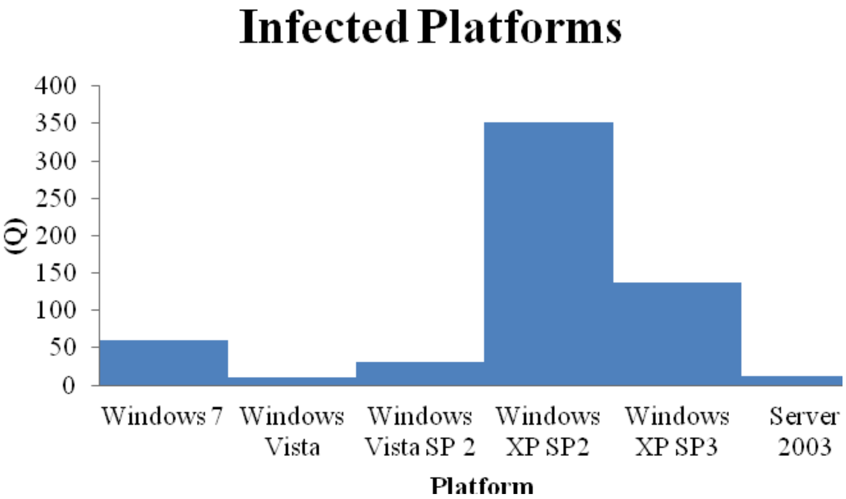
2.3 TRENDS AND EMERGING CAPABILITIES

1. 'Boutique' Botnets evade current detection capabilities
2. External BI system interaction provides intelligence in asset ranking & tasking
4. RingO bootkits will dramatically lengthen compromise
5. Radical shift in time distribution affects Deterrence

3.BACKGROUND

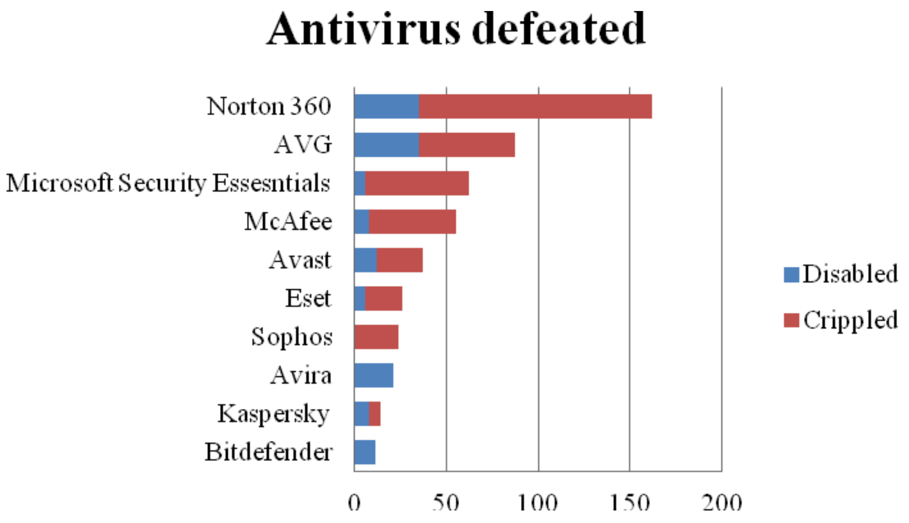
3.1 INFECTED PLATFORMS

All of the infected platforms were based on Microsoft Windows. They varied from Windows XP to Server
2003.



3.2ANTIVIRUS PLATFORMS DEFEATED - %100

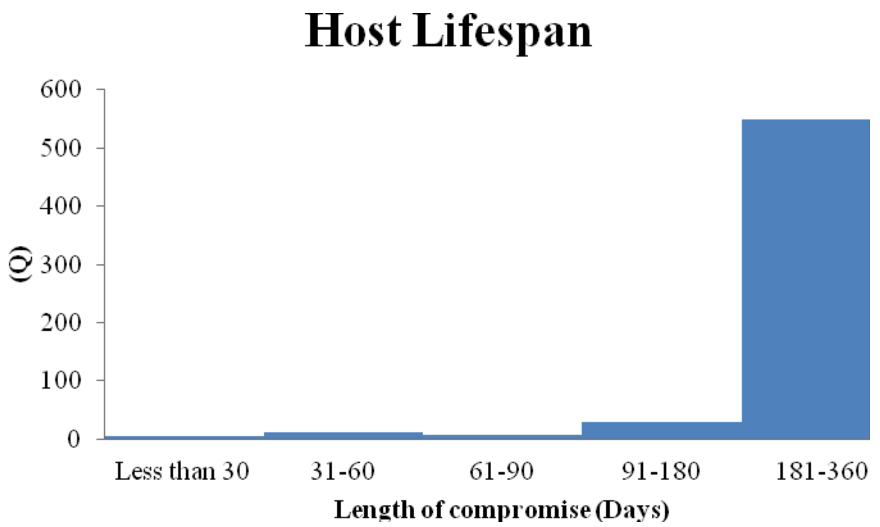
While 104 computers did *not* have antivirus software installed, 499 did. In these cases all ten different vendor products were defeated, being either disabled or crippled.



Disabled; *Certain capabilities disabled such as active protection and updates*
Crippled*; Major capabilities still appeared operational but no longer functioned, or operated in diminished capacity*

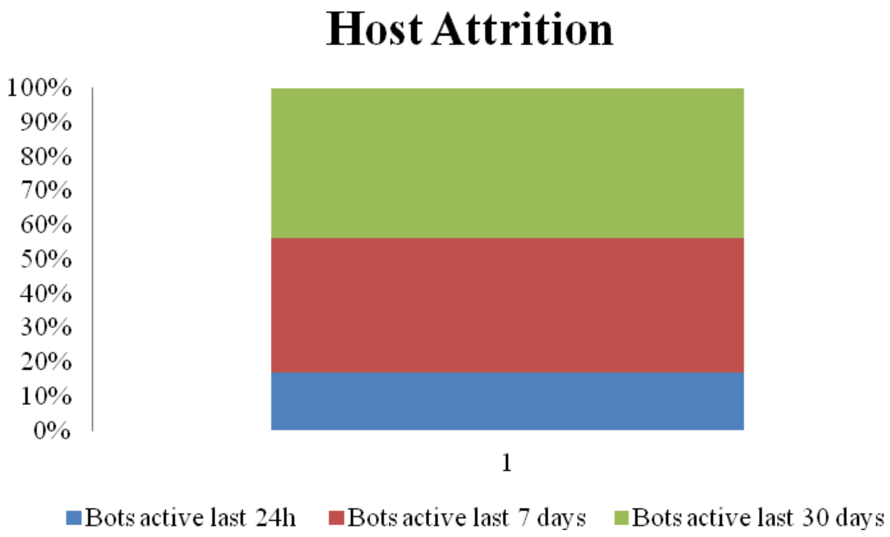
3.3 HOST LIFESPAN

The median lifespan of the infection (effective compromise) for the computers was 243 days, or 8 months



3.4 HOST ATTRITION

There was no evidence of meaningful attrition. %89 were active within the previous 7 days, %100 were active within 30.



3.5 MALWARE CAPABILITIES

Seven primary capabilities were available

1. Credential capturing targeting specific E-Commerce websites
2. Interception of both HTTP and HTTPS traffic
3. HTML Form data grabber
4. Full Remote Desktop Access to Computer (CyberGate, BackOrifice)
5. Screenshots
6. Internet Use (browser history)
7. Interception of FTP and POP3 connections

3.6 MALWARE DEFENSES

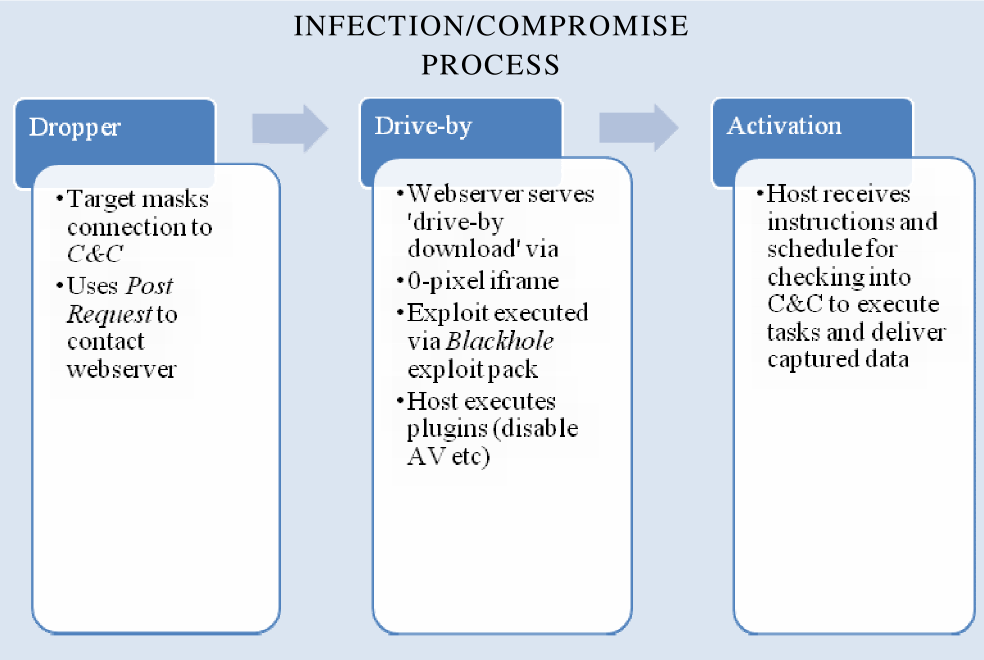
Eight primary defensive capabilities were available

1. Disabling of anti-virus protection using running process identification
2. Crippling of anti-virus protection *(blackhole updates)*
3. Prevention of application & system updates *(blackhole updates)*
4. Storage of captured credentials in CAB files to reduce detection
5. Anti-Analysis mechanism (*Strings are obfuscated in memory and only decoded when they are used, making static analysis difficult. Also, additional fake 'instructions are inserted at infrequent intervals to make reverse engineering difficult.)*
6. Polymorphic encryption
7. Communications to C&C encrypted with RC4
8. Detects and disinfects other malware/botnets *(ZeuS. Limbo, ImageFile Execution, Barracuda, BlackEnergy, MyLoader, Adrenalin, Genertic)* via the MiniAV plugin

3.6 INFECTION/COMPROMISE PROCESSES

Posted via Blog websitea and SEO Poisoning

3.7.1| DRIVE-BY



INFECTION/COMPROMISE PROCESS

Dropper
- Target masks connection to *C&C*
- Uses *Post Request* to contact webserver

Drive-by
- Webserver serves 'drive-by download' via
- 0-pixel iframe
- Exploit executed via *Blackhole* exploit pack
- Host executes plugins (disable AV etc)

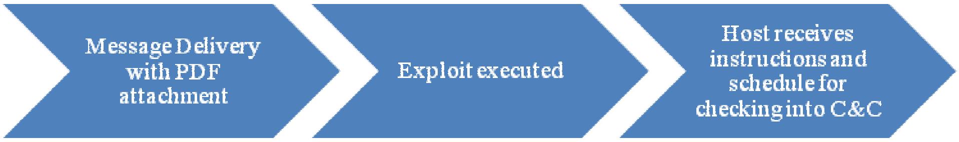
Activation
- Host receives instructions and schedule for checking into C&C to execute tasks and deliver captured data

Blackhole kit exploited primarily java vulnerabilities;

- JS/Exploit.JavaDepKit (CVE-2010-0886)
- Java/Exploit.CVE-2011-3544
- Java/Exploit.CBE-2012-0507
- Java/Agent

3.7.2| MESSAGING - EMAIL

PDF attachments with names and logos of organizations such as Commerce Bank, UMB, HR Block, Cerner Health Systems, Garmin and Yellow Freight. Attachment names combined a company name with ‘Statements”, “Invoices” and ‘Payment Due’



Message Delivery with PDF attachment

Exploit executed

Host receives instructions and schedule for checking into C&C

PDF Exploits List Goes Here

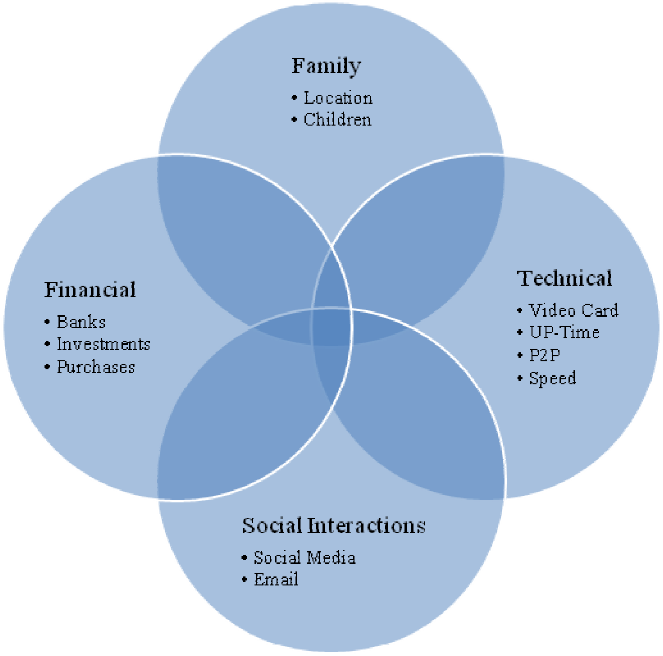
4. NEW CAPABILITIES

4.1 USE OF LINKAGE ANALYSIS AND EXTERNAL BI PLATFORM TO DETERMINE ASSET VALUE & TASKING

While no direct evidence of a comprehensive analysis capability was discovered on the *Carberp* C&C platform itself the type and structure of the collected information provides strong evidence that an external engine (multidimensional analysis) was used to analyze the data to find patterns and linkages in behavior and be directly applied to make intelligent decisions on asset tasking and execution. To that end two calculated values; *Confidence* and *Asset Task* were discovered on the C&C interface itself.

It is our belief that the collected data was used to classify and rank the assets (compromised computer) to build a profile, or "Identity" of individuals and entire families. Criteria included what they use computers for, where they live, who they correspond to and what kind of activities and interests they have. The more an individual or family used computers for communication and daily tasks, the more they reflected the identity of the owner and enabled a higher confidence ranking.

On this particular *Carberp* botnet the malware performed surveillance on its 'slaved computers' for an average of eight months. During the eight month period information regarding technical capabilities, social interactions, personal or family unit and financial was gathered.



While the calculated values did not yield the operations themselves, there was enough data to attempt to attempt to reverse engineer the calculations. In order to test this theory a multi-dimensional analysis dataset using the open source Pentaho's Online Analytical Processing Mondrian server to replicate the calculated values and asset tasking results

The result matched the ratings based on the following criteria.

The values and relationships created were;

1. Confidence value is directly related to the time distribution of infection.
2. MO of activities generated based on confidence, frequency of activities over time
3. Asset tasking based on Financial, Social, Technical and Family categories
4. Asset tasking groups increased value based on geography (across state lines)
5. Length of time is the leading criteria; the worth is increased based on time, rather than a size "value"

Detailed documentation of the OLAP dataset and techniques will be made available in a separate dedicated document

4.2 ADVANCED ENCRYPTION & OBFUSCATION TECHIQUES ARE HIGHLY EFFECTIVE

The malware defeated and evaded detection from ten antivirus vendors. Five capabilities were used;

1. Storage of collected information in CAB files
2. Use of encrypted C&C communications
3. Encryption of plug in downloads
4. 'Update' allows regular updates to prevent AV reverse engineers from detecting each build
5. Adds random bytes to dropped files to evade static AV signatures

While the *Carberp* malware continues to be developed technically increasing its technical capabilities and evasion techniques. The more interesting

4.3 'MODULAR, PLUG & PLAY WARE

While the Carberp malware continues to develop technically increasing its technical capabilities and evasion techniques

At the CARO 2012 WWWTF ESET and GroupB presented 'Carberp Evolution and Blackhole, Investigation Beyond the Event Horizon' in which they explored Russian cybercrime groups use of *Carberp* and three different significant strains with advanced capabilities; Gizmo, D****** and Hodprot

Of the three Hodprot seemed to be the most advanced, integrating not only the 'DeletePatch' functionality but the capability of delivering Ring0 level boot kits.

DDOS	• Download DDOS plugin and start attack
Update	• Update new version of Carberp
Loaddll	• download plugin and load into memory
Bootkit	• **download and install bootkit (Ring0)**
UpdatePatch	• download and modify java runtime
DeletePatch	• delete java runtime modifications

Ring0 level bootkits are the holy grail of infections/compromises and could theoretically generate indefinite compromise time periods.

5. TRENDS & EMERGING CAPABILITIES

5.1 'BOUTIQUE' BOTNETS ARE DESIGNED TO EVADE DETECTION CAPABILITIES

The investigation yielded no evidence of international involvement commonly found among larger botnets which, in most cases, can be traced back to .ru or other foreign domains. Instead the botnet used dynamic DNS entries based on .com and .biz domains hosted in the US.

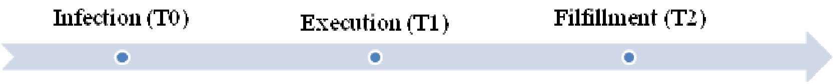
There also did not appear to be a general push to obtain a larger population as evidenced by the low attrition and static population.

Infections were distributed based on exploits delivered by PDFs and blogsites (Java via Blackhole) using *regional* Financial Institutions and Retailers names and brand recognition. PDF attachments with names and logos of organizations such as Commerce Bank, UMB, HR Block, Cerner Health Systems, Garmin and Yellow Freight. Attachment names combined a company name with 'Statements", "Invoices" and 'Payment Due'

When combining the specific geographical and regional target, the specific compromise channels and techniques, size constraints, technical evasion capabilities and advanced intelligence-decision analysis capabilities, a case could be made that a smaller, more intelligent botnet could increase the assurance of long-term viability and ultimately have a greater value than their larger relatives.

5.2 RADICAL SHIFT IN TIME DISTRIBUTION AFFECTS DETERRENCE

The extended period of surveillance and resources placed on analysis demonstrates that significant value is being placed on the development of long-term assets. The direct relationship between confidence and the time distribution of infection proves that long-term assets are perceived as more valuable than quicker fulfillment activities such as advanced fee scams and bank transfer fraud.



This is a reversal of the traditional fraud decision model in which confidence (C) decreased as time passed between fraud execution (T1) and fulfillment (T2)

$$C = \frac{1}{T2 - T1}$$

Instead the confidence value is now based on the time between initial infection (T0) and the point of fraud execution (T1). This significantly decreases the traditional deterrence mechanisms associated with the perpetrator's perception of the "Fix'.

$$C = T0 + T1$$

This change the fraud decision model could not occur without the technical assurances that assets will remain undetected and compromised for extended periods of time. While the current technology, and 'boutique' style deployments limits detection efforts emerging capabilities such as Ring0 level bootkits and obfuscation will allow the compromise time to extend indefinitely, not only increasing the effectiveness of current fraud but allowing more sophisticated and deliberate fraud activities to occur.

A successful transition to strategic objectives will place considerable strain on internet-based transactions, trusted access and identify management.

BIBLIOGRAPHY

Carberp Evolution and Blackhole, Investigation Beyond the Event Horizon presented at the 2012 Caro WWWTF by ESET and GroupB . Sourced from http://blog.eset.com/2012/05/24/carberp-gang-evolution-at-caro-2012

Linkage Analysis (Labuschagne) 5 Steps
1 Obtain data from multiple sources; 2, Reviewing the data and identifying significant features across the series; 3, Classifying significant features as either MO or ritualistic; 4, Comparing combination of MO and Fantasy across series to determine if signature exists; 5, Compiling a written report

Sourced from http://en.wikipedia.org/wiki/Behavioral_Analysis_Unit