Malware Analysis and Adversary Infrastructure Mapping: **the One-Two Punch**

JUNE 2016

DOMAINTOOLS

Meet Your Presenter

#DTWEBINAR

Tim Helming, Director of Product Management

- 15+ years in infosec
- Passionate about fighting bad guys…
- …and about other stuff too ☺

Alissa Torres, Certified SANS Instructor

- Digital Forensics/Incident Response Consultant
- SANS Course Author, Track Lead

Punch One: Malware Hunting and Analysis

DOMAINTOOLS

Detection of Infected Host

DOMAINTOOLS

All detected items

Items that were detected on your PC.

Detected item	Alert level	Date
Trojan:Win32/Malex.gen!E	Severe	6/14/2016

Category: Trojan

Description: This program is dangerous and executes commands from an attacker.

Recommended action: Remove this software immediately.

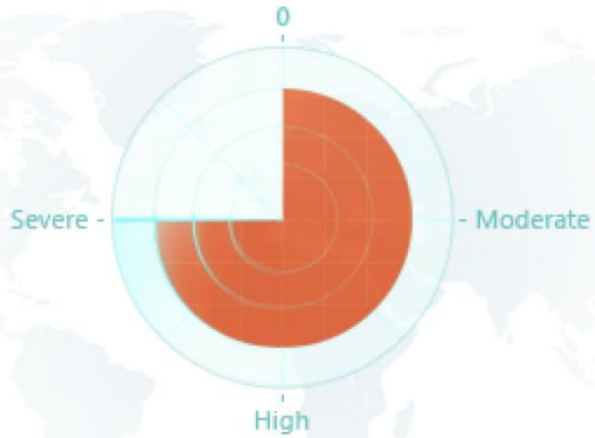
Items:
file:C:\Users\possiblyothers\AppData\Local\Temp\svchost.exe
file:C:\Users\POSSIB~1\AppData\Local\Temp\svchost.exe

Detection of Infected Host

DOMAINTOOLS

Trojan: Win32/Malex.gen!E

Also detected as: Trojan.Win32.Agent.cjgo (Kaspersky), Trojan.Agent.LKTH (VirusBuster), Trojan.Generic.1614223 (BitDefender), Win32/PSW.Sagic.15.E (ESET), Spy-Agent.dt (McAfee), :Trj/Agent.MDR (Panda),



Trojan:Win32/Malex.gen!E
Alert level: **Severe**

First published: Jun 30, 2009
Latest published: Jul 26, 2010

Summary | What to do now | Technical information | Symptoms

Trojan:Win32/Malex.gen!E is a generic detection for certain malicious files that attempt to copy itself in certain folders without the user's consent or knowledge.

Triage/Volatile Data Collection

DOMAINTOOLS

- ☑ Physical Memory Acquisition
- ☑ Autoruns Collection
- ☑ Windows OS Artifacts
- ☑ Network Traffic Capture

DOMAINTOOLS

Process List

Name	PID	PPID	Sess	Wow64	Start
svchost.exe	656	556	0	0	2016-06-12 15:53:07
svchost.exe	708	556	0	0	2016-06-12 15:53:07
svchost.exe	856	556	0	0	2016-06-12 15:53:10
svchost.exe	904	556	0	0	2016-06-12 15:53:10
svchost.exe	1020	556	0	0	2016-06-12 15:53:13
svchost.exe	8	556	0	0	2016-06-12 15:53:13
svchost.exe	828	556	0	0	2016-06-12 15:53:15
svchost.exe	884	556	0	0	2016-06-12 15:53:18
svchost.exe	360	556	0	0	2016-06-12 15:53:18
svchost.exe	1512	556	0	0	2016-06-12 15:53:25
svchost.exe	1184	556	0	0	2016-06-12 15:53:39
svchost.exe	2436	556	0	0	2016-06-12 15:54:48
svchost.exe	720	556	0	0	2016-06-12 17:50:16
svchost.exe	3524	556	1	0	2016-06-13 11:41:09
svchost.exe	4616	2044	1	1	2016-06-13 11:56:00

DOMAINTOOLS

SVCHOST Process Details

```
0xffffe001a9a16780:svchost.exe                    4616   2044      5      0 20
UTC+0000
   audit: \Device\HarddiskVolume2\Users\POSSIB~1\AppData\Local\Temp\svchost.exe
   cmd: C:\Users\POSSIB~1\AppData\Local\Temp\svchost.exe
   path: C:\Users\POSSIB~1\AppData\Local\Temp\svchost.exe
```

- Anomalous Path
- Wrong Parent
- Late Creation Time

DOMAINTOOLS

Extracted SVCHOST Binary Strings

```
…
0123456789ABCDEF
.locky
\_Locky_recover_instructions.txt
\_Locky_recover_instructions.bmp
Open
svchost.exe
:Zone.Identifier
vssadmin.exe Delete Shadows /All /Quiet
Locky
cmd.exe /C del /Q /F ”
_Locky_recover_instructions.bmp
_Locky_recover_instructions.txt
Winnt
Application Data
…
```

DOMAINTOOLS

Extracted SVCHOST Binary

virustotal

SHA256: 787cea08c6a10fdc2558b0b8d31ec6aa66afb150e08996c1be1dda39cdd640d5

File name: executable.4616.exe

Detection ratio: 25 / 48

Analysis date: 2016-06-15 03:44:39 UTC (1 minute ago)

0 0

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
Ad-Aware	Gen:Variant.Graftor.272655	20160615
AhnLab-V3	Trojan/Win32.Locky	20160614
Antiy-AVL	Trojan[Ransom]/Win32.Locky.genb	20160615

DOMAINTOOLS

Network Connections

B	C	D	E
Proto	LocalAddr	ForeignAddr	State
TCPv4	172.16.7.54:50257	208.100.26.234:80	CLOSE_WAIT
TCPv4	172.16.7.54:50302	13.107.4.50:80	CLOSED
TCPv4	172.16.7.54:50235	63.146.14.9:443	CLOSED
TCPv4	172.16.7.54:50293	64.4.54.18:443	ESTABLISHED
TCPv4	172.16.7.54:50268	23.218.204.183:443	ESTABLISHED
TCPv4	172.16.7.54:50205	204.79.197.200:443	CLOSED
TCPv4	172.16.7.54:50260	86.104.134.144:80	CLOSED
TCPv4	172.16.7.54:50244	208.100.26.234:80	CLOSED
TCPv4	172.16.7.54:50204	204.79.197.200:443	CLOSED
TCPv4	172.16.7.54:50258	86.104.134.144:80	SYN_SENT
TCPv4	172.16.7.54:50233	63.146.14.9:443	CLOSED
TCPv4	172.16.7.54:50100	65.52.108.225:443	ESTABLISHED
TCPv4	172.16.7.54:50231	63.146.14.9:443	CLOSED
TCPv4	172.16.7.54:50297	13.107.4.50:80	ESTABLISHED

B	C	D	E
Proto	LocalAddr	ForeignAddr	State
TCPv4	172.16.7.54:50257	208.100.26.234:80	CLOSE_WAIT
TCPv4	172.16.7.54:50244	208.100.26.234:80	CLOSED
TCPv4	172.16.7.54:50247	208.100.26.234:80	CLOSED

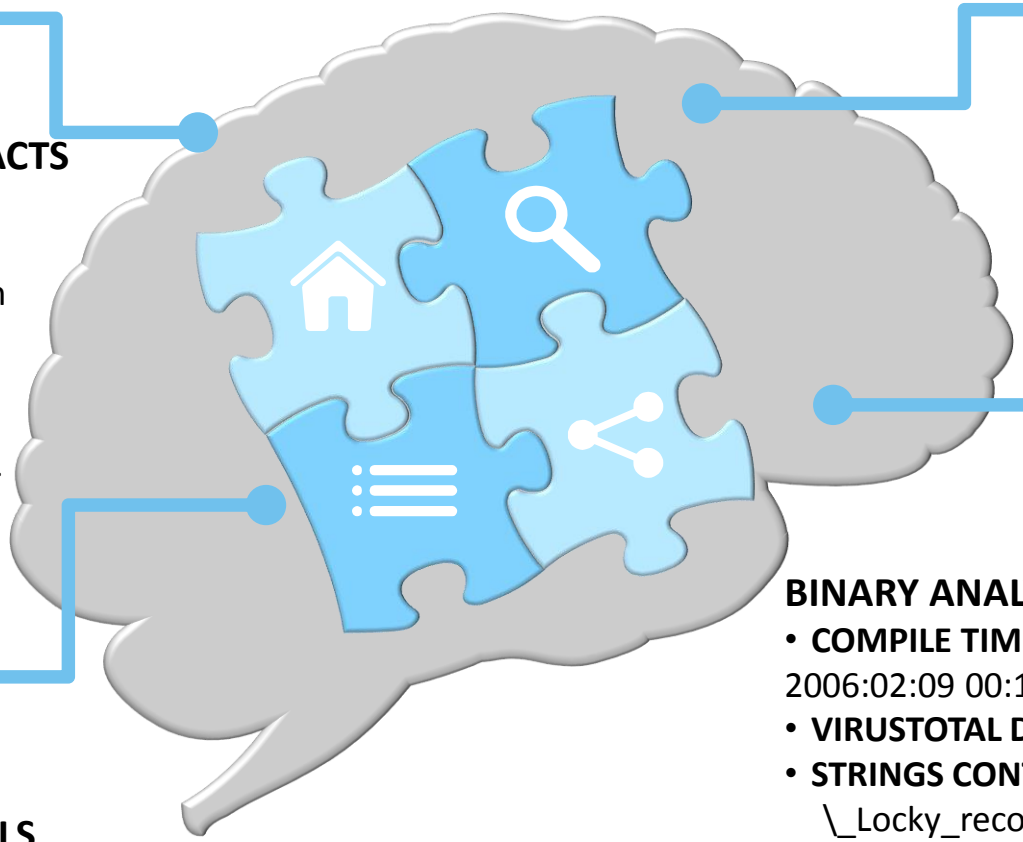
DOMAINTOOLS

Packet Carving from Memory

Source	Destination	Protocol	Length	Info
172.16.7.54	172.16.0.1	DNS	72	Standard query 0x787c A ssl.bing.com
172.16.7.54	172.16.0.1	DNS	72	Standard query 0x787c A ssl.bing.com
172.16.0.1	172.16.7.54	DNS	148	Standard query response 0x787c CNAME ssl-bing-com.
172.16.0.1	172.16.7.54	DNS	148	Standard query response 0x787c CNAME ssl-bing-com.
172.16.7.54	172.16.0.1	DNS	77	Standard query 0x893c A vdijrsjcnnxftd.de
172.16.7.54	172.16.0.1	DNS	77	Standard query 0x893c A vdijrsjcnnxftd.de
172.16.0.1	172.16.7.54	DNS	129	Standard query response 0x893c No such name
172.16.7.54	172.16.0.1	DNS	76	Standard query 0x777d A npkjhnfbnlgmf.in
172.16.0.1	172.16.7.54	DNS	129	Standard query response 0x893c No such name
172.16.7.54	172.16.0.1	DNS	76	Standard query 0x777d A npkjhnfbnlgmf.in
172.16.0.1	172.16.7.54	DNS	141	Standard query response 0x777d No such name
172.16.7.54	172.16.0.1	DNS	68	Standard query 0x2257 A enerf.nl
172.16.0.1	172.16.7.54	DNS	141	Standard query response 0x777d No such name
172.16.7.54	172.16.0.1	DNS	68	Standard query 0x2257 A enerf.nl
172.16.0.1	172.16.7.54	DNS	139	Standard query response 0x2257 No such name
172.16.7.54	172.16.0.1	DNS	71	Standard query 0x14ad A rdbbnojt.fr
172.16.7.54	172.16.0.1	DNS	71	Standard query 0x14ad A rdbbnojt.fr
172.16.0.1	172.16.7.54	DNS	131	Standard query response 0x14ad No such name
172.16.7.54	172.16.0.1	DNS	70	Standard query 0xc9ec A jstfqmo.it
172.16.7.54	172.16.0.1	DNS	70	Standard query 0xc9ec A jstfqmo.it
172.16.0.1	172.16.7.54	DNS	131	Standard query response 0x14ad No such name
172.16.0.1	172.16.7.54	DNS	139	Standard query response 0x2257 No such name
172.16.0.1	172.16.7.54	DNS	125	Standard query response 0xc9ec No such name
172.16.7.54	172.16.0.1	DNS	73	Standard query 0x2162 A wfdrdiolrq.pw
172.16.7.54	172.16.0.1	DNS	73	Standard query 0x2162 A wfdrdiolrq.pw
172.16.0.1	172.16.7.54	DNS	89	Standard query response 0x2162 A 208.100.26.234
172.16.0.1	172.16.7.54	DNS	89	Standard query response 0x2162 A 208.100.26.234
172.16.0.1	172.16.7.54	DNS	125	Standard query response 0xc9ec No such name

Memory Analysis of Infected Host

DOMAINTOOLS



NETWORK ARTIFACTS

- **DNS REQUESTS:**
  vdijrsjcnnxftd.de
  npkjhnfbnlgmf.in
  enerf.nl
  rdbbnojt.fr
  jstfqmo.it
  wfdrdiolrq.pw -> RESOLVED TO **208.100.26.234**

TIMELINE ANALYSIS

- Initial execution preceded by opening an email with **SUBJECT LINE: ATTACHED IMAGE**

PROCESS DETAILS

- **PATH:** %USERPROFILE%\APPDATA\LOCAL\TEMP\SVCHOST.EXE
- **INITIAL EXECUTION:** 2016-06-13 11:56:00 UTC

BINARY ANALYSIS

- **COMPILE TIME:** 2006:02:09 00:15:40UTC
- **VIRUSTOTAL DETECT: 25/48**
- **STRINGS CONTAIN:**
  _Locky_recover_instructions.txt
  _Locky_recover_instructions.bmp
  svchost.exe
  vssadmin.exe Delete Shadows /All /Quiet
  cmd.exe /C del /Q /F "

Punch Two: Mapping and Blocking Malicious Infrastructure

DOMAINTOOLS

The Bridge…

…Between malware analysis and infrastructure mapping

Malware has to do “stuff” that involves the Internet

- Phone home to C2 for instructions
- Exfiltrate data
- Get encryption key (ransomware)
- etc…

And the most effective way for it to find the hosts it needs to talk to is via *domain names*.

Discover/Expand/Block

To (over)simplify:

- Start with a domain name (malware infra in this case)
  - Block it
- Find what it’s connected to
  - Block those
- Determine if it’s been active previously
  - Search logs

A Typical Hunt Sequence

DOMAINTOOLS

HOW DO THE STEPS PLAY OUT?

An indicator is seen

IOC Sources:
- Phish domain
- Firewall/IPS alert
- **Malware Analysis**

Form Hypothes(es)

This indicator could be
- Part of a campaign
- Targeting my industry
- Targeting my org

Gather Data

Enrich indicators
- Cross-indexed Whois/DNS data
- Other domain profile info

Test Hypotheses

Evaluate data
- Connected domains?
- Thematic consistency?
- High risk scores?
- Other red flags?

Test Hypotheses part 2

Look for more evidence
- Search alerts for domains/IPs
- Search archived logs
- Search SIEM/feeds

Act!

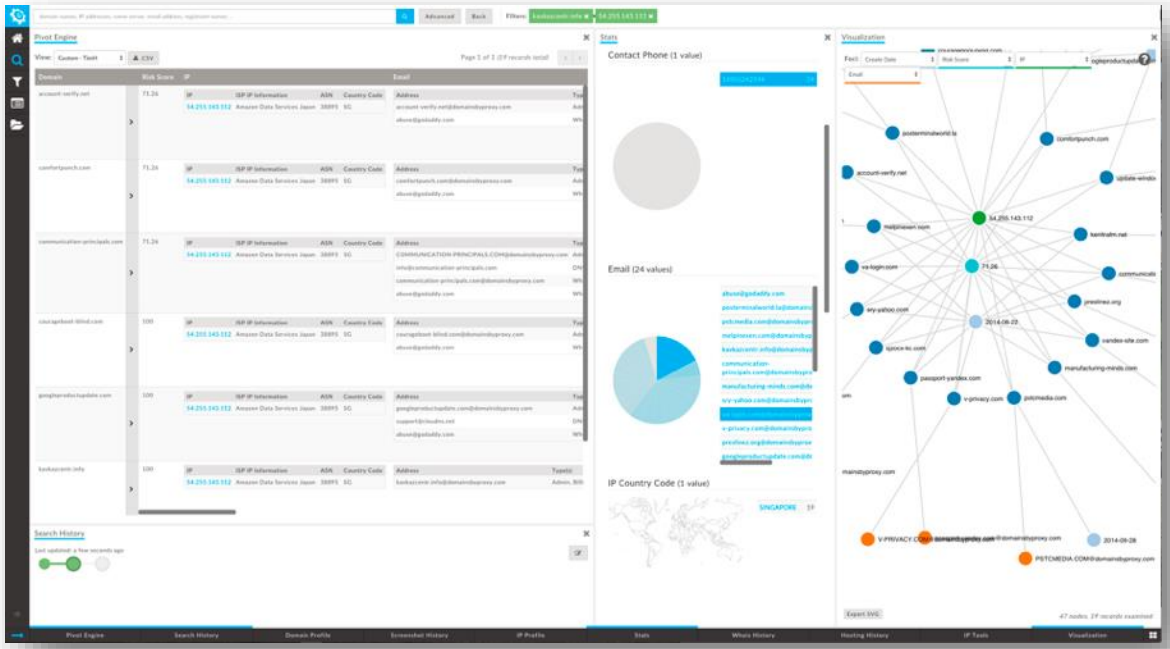
- Block domains/IPs in network/host defenses
- Monitor observed actors
- Block future infrastructure

DomainTools Iris

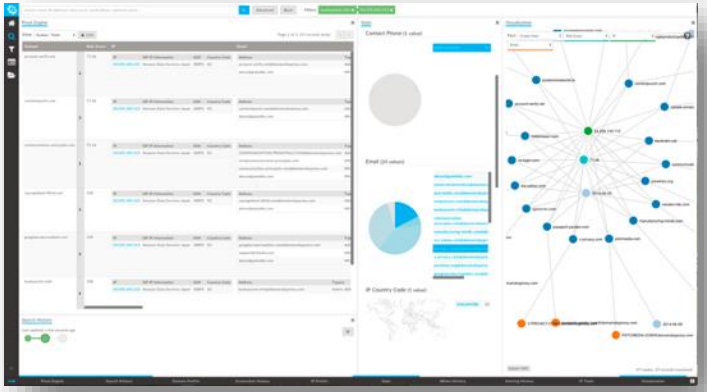
FLAGSHIP DOMAIN/DNS INVESTIGATION PLATFORM

Easy mining of DomainTools databases for cyber investigations and related research activities

- Whois, DNS, MX, and more—all cross-referenced
- Historical Whois and DNS data
- Based on research into real-world investigative workflows



Scientific Method for Investigations



DEMO TIME!

The Proof is in the Data

DOMAINTOOLS

OUR DATA

300 Million
Current domain names

100+ Million
ccTLD domains

10+ Billion
Current Hostnames

10+ Million
Continually mapped IPv4 address range delegations and sub-delegations

15+ Million
DNS data points on changes among domain names, IP addresses, name servers and Registrants

10+ Billion
Historical domain profile records on over nearly 500 million current and previously registered domain names

5,000,000
Nearly 5 Million new domain profiles captured daily

1,000,000
Over 1 Million new website screenshots taken daily

20,000,000
Nearly 20 Million new domain-IP resolutions

Current Product and Solution Suite

DomainTools Iris – unified domain and DNS research tool

Enterprise-grade APIs

- Integration with third-party products
- Partnerships with threat intelligence platforms
- Large-scale enrichment, expansion & automation

Monitoring products for brands, IPs, NSs & registrants

Domain Reputation Engine

Investigative tools for domains, IPs, NSs & registrants

DOMAINTOOLS

QUESTIONS?

sales@domaintools.com

product@domaintools.com

@domaintools

@timhelming