

Fighting Back Malware with IOC & YARA

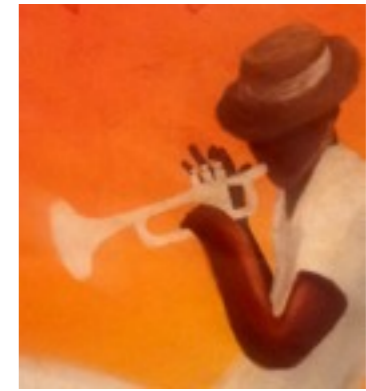
OSSIR Paris, 2012.12.11

Saâd Kadhi, saad.kadhi@hapsis.fr

HAPSIS

<http://www.hapsis.fr/>

Speaker Bio



@_saadk

- Saâd Kadhi
- CTO at HAPSI, GCIH, GCFA
- 14y+ of infosec experience, almost 5y in Digital Forensics & Incident Response
- Apt walker, apt swimmer & apt music fan :-)
- 0x0ORGANICF00D

Agenda

- The Threat Landscape
- Fighting Back
- YARA
- IOC
- Closing Thoughts

The Threat Landscape

Source: <http://attrition.org/security/conferences/2012-BruCON-CyberWar-v18-FINAL03.pptx>



We are APT
We are Legion

A Quick Overview

- What we (old timers) used to call ‘targeted attacks’ is now dubbed APT
- Media circled over this new term like vultures on carrion
- Media attention is good, media attention is bad

Caution!

- Media & others (over)sells APT for fun, profit but mainly for profit
- Instill fear or... overhype real security incidents
- Think different: who says what? For what purpose (vested interest)?
- It was, is & will still be a foggy mine field

Things could easily have gone a different way.

Those behind the attacks also made no secret of their compromise: publishing public statements on their attack and the addresses of compromised systems online - not typical of APT-style attacks.

Beyond that, clues in the malware cast doubt on Iran as the source of Shamoon.

As the New York Times [reported](#), the code of the malware refers to the "Arabian Gulf," rather than the "Persian Gulf" - the term of choice for Iranians

The evidence of links to Iran in the Shamoon/Aramco attack were "largely circumstantial," Bloomberg reported, citing interviews with U.S. intelligence officials.

That makes it all the stranger that Defense Secretary Leon Panetta, speaking at a conference for Business Executives for National Security in New York on October 11th, called Shamoon a "very sophisticated tool" and cited the Aramco incident as evidence of the danger of a "Cyber Pearl Harbor." (A phrase, by the way, that [many deem tasteless](#))

The Shamoon attack, Panetta said, and a subsequent attack on the Qatari firm RasGas was one of the most destructive to date and underscored both advances in malware and the increase in threats to businesses from sophisticated "cyber actors."



The sad truth may be that cyber security is now a new front in a very old Washington DC parlor game, namely: hyping the threat.

Panetta's clear goal in his speech wasn't to warn about the dangers of malware, per se, or even targeted attacks. Instead, it was to talk up the need for comprehensive cyber security legislation that's been blocked in Congress because of election-related gridlock.

In his speech, Panetta [argued](#) that private firms like Aramco don't have the resources to battle such sophisticated threats alone, he said, underscoring the need for greater public-private partnerships - but that new legislation like the pending CISPA act were needed to enable such collaboration.



Eugene Kaspersky ✓

@e_kaspersky



Follow

Iran behind Shamoon Attack
issource.com/iran-behind-sh... <- Don't
think so. Iranians would never refer to
Persian Gulf as "Arabian Gulf"

Reply Retweeted Favorited More

55
RETWEETS

8
FAVORITES



7:31 AM - 19 Oct 12 · Embed this Tweet

#IFDEF

apt | apt |

adjective

1 appropriate or suitable in the circumstances: *an apt description of her nature.*

2 [predic.] (**apt to do something**) having a tendency to do something: *she was apt to confuse the past with the present.*

3 quick to learn: *he proved an apt scholar.*

DERIVATIVES

apt·ly adverb

ORIGIN late Middle English (in the sense ‘*suited, appropriate*’): from Latin *aptus* ‘*fitted*,’ past participle of *apere* ‘*fasten*.’

Some Examples



Speaking of Security

The Official RSA Blog and Podcast



Topics

Administration

Authentication

Automation

Big data

Cloud Security

Compliance

Consumer Security

Cryptography

Cyber Security Training

Anatomy of an Attack

Written on 2011/04/01 by Uri Rivner

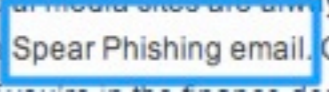
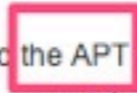
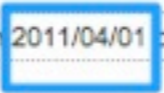
Comments (44)

I was on a tour in Asia Pacific when I first heard the [news](#) about the attack. The investigation into this attack continues but I'm eager to share some information with you about it.

Let's first make sure everyone is on the same [page](#). The number of enterprises hit by APTs grows by the month; and the range of APT targets includes just about every industry. Unofficial tallies number dozens of mega corporations attacked; examples are in the press regularly, and some examples are [here](#), and [here](#).

These companies deploy any imaginable combination of state-of-the-art perimeter and end-point security controls, and use all imaginable combinations of security operations and security controls. Yet still the determined attackers find their way in. What does that tell you?

The first thing actors like those behind the APT do is seek publicly available information about specific employees – social media sites are always a favorite. With that in hand they then send that user a Spear Phishing email. Often the email



The attacker in this case sent two different phishing emails over a two-day period. The two emails were sent to two small groups of employees; you wouldn't consider these users particularly high profile or high value targets. The email subject line read "2011 Recruitment Plan."

The email was crafted well enough to trick one of the employees to retrieve it from their Junk mail folder, and open the attached excel file. It was a spreadsheet titled "2011 Recruitment plan.xls."

The spreadsheet contained a zero-day exploit that installs a backdoor through an Adobe Flash vulnerability (CVE-2011-0609). As a side note, by now Adobe has released a [patch](#) for the zero-day, so it can no longer be used to inject malware onto patched machines.

Bits

NOVEMBER 30, 2012, 4:09 PM | 26 Comments

Study May Offer Insight Into Coca-Cola Breach

By NICOLE PERLROTH

FACEBOOK

TWITTER

GOOGLE+

SAVE

E-MAIL

SHARE

PRINT

Spend enough time with cybersecurity experts and chances are you will hear some variation of this line: There are two types of companies in the United States, those that have been hacked and those that don't yet know they've been hacked.



Jewel Samad/Agence France-Presse — Getty Images

Government intelligence officials and cybersecurity specialists say hackers — predominantly from China — are siphoning gigabytes, if not terabytes, of data from companies in the United States every day. We count on much of this information to deliver the innovative products and services that will lead to new jobs and economic growth. The security software company [McAfee estimates](#) that in 2008 alone, companies around the world lost more than \$1 trillion because of this sort of intellectual property theft.



CASE STUDY: FORTUNE 500 MANUFACTURING COMPANY

In 2009, a U.S.-based Fortune 500 manufacturing company initiated discussions to acquire a Chinese corporation. During the negotiations, APT attackers compromised computers belonging to the executives of the U.S.-based company, most likely in an effort to learn more details of the negotiations. Sensitive data left the company on a weekly basis during negotiations, potentially providing the Chinese company with visibility to pricing and negotiation strategies.

Law enforcement notified the company of the intrusion into their networks. The APT had targeted executives involved in direct talks with the Chinese corporation. Law enforcement provided the victim organization with proof that the APT had exfiltrated critical e-mails containing details of the negotiation from the victim organization's executives just days prior to the negotiations.

The attackers compromised multiple key executives' systems. The APT initially sent targeted, spear phishing e-mails to four company executives. The e-mail was crafted to look like it originated from a fellow employee and discussed a message from the CEO on conserving resources. One of the key executive's systems was compromised when he clicked on the link embedded within the e-mail, which then downloaded and executed a malicious file. The malicious file installed a fully functional command and control backdoor on their system that allowed the APT full access to the system from the Internet.

The APT copied malware to the executive's system. From there, the APT used password-stealing utilities to gain access to new systems on the network. The APT

South Carolina Offers Details of Data Theft and Warns It Could Happen Elsewhere

By [ROBBIE BROWN](#)

Published: November 20, 2012

ATLANTA — Gov. [Nikki R. Haley](#) said on Tuesday that South Carolina officials had not done enough to stop computer hackers who recently stole millions of personal financial records.

Connect With Us on Twitter

Follow

@NYTNational for breaking news and headlines.

Twitter List: Reporters and Editors



A new report shows that outdated computers and security flaws at the state's Department of Revenue allowed international hackers to steal 3.8 million tax records, the governor said. She announced that the agency's director, James Etter, would resign at

the end of the year.

"Could South Carolina have done a better job? Absolutely," she said. "We did not do enough."

Experts say the cyberattack, which resulted in the theft of 3.8 million [Social Security](#) numbers and 387,000 credit and debit card numbers, was the largest ever against a state government agency.

On Tuesday, the computer security firm [Mandiant](#) released a report with new details about the attack. Hackers broke into the agency's computer system by sending state employees spam e-mail that contained an embedded link. If employees clicked on the link, software was activated on their computers that stole their user names and passwords.

FACEBOOK

TWITTER

GOOGLE+

SAVE

E-MAIL

SHARE

PRINT

REPRINTS

Summary of the Attack

A high level understanding of the most important aspects of the compromise are detailed below.

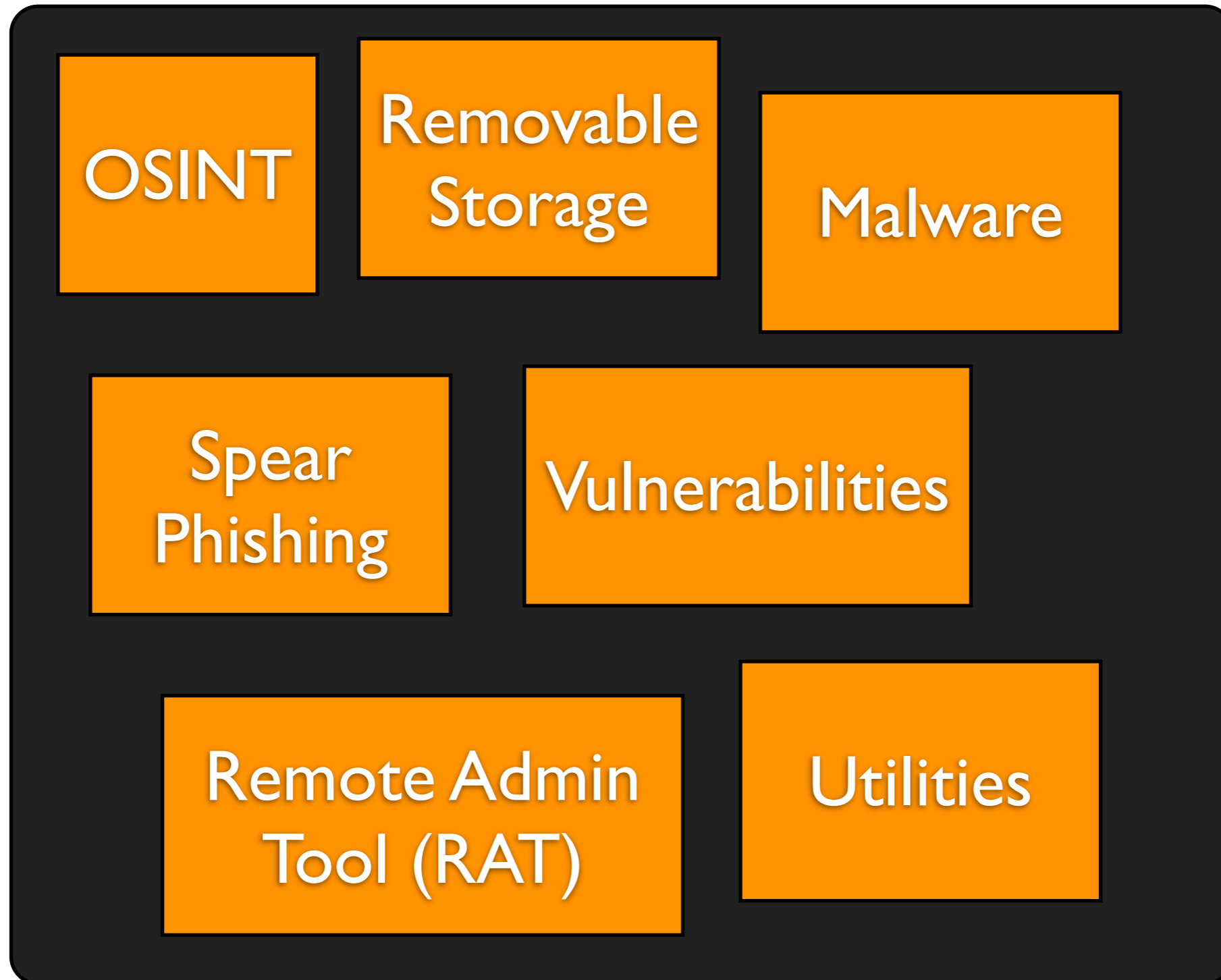
1. August 13, 2012: A malicious (phishing) email was sent to multiple Department of Revenue employees. At least one Department of Revenue user clicked on the embedded link, unwittingly executed malware, and became compromised. The malware likely stole the user's username and password. This theory is based on other facts discovered during the investigation; however, Mandiant was unable to conclusively determine if this is how the user's credentials were obtained by the attacker.

Extent of Compromise

The following points describe the extent of the compromise:

1. The attacker compromised a total of 44 systems:
 - One system had malicious software ("backdoor") installed
 - Three systems had database backups or files stolen
 - One system was used to send data out of the environment to the attacker
 - Thirty nine systems were accessed by the attacker (the attacker performed such activities as reconnaissance and password hash dumping)
2. The attacker used at least 33 unique pieces of malicious software and utilities to perform the attack and data theft activities including:
 - A backdoor
 - Multiple password dumping tools
 - Multiple administrative utilities
 - Multiple Windows batch scripts to perform scripted actions
 - Multiple generic utilities to execute commands against databases

#IFDEF (reloaded)



#IFDEF (reloaded)

APT

OSINT

Removable
Storage

Malware

Spear
Phishing

Vulnerabilities

Remote Admin
Tool (RAT)

Utilities

More Caution!

- Attribution is difficult
- Things can get messy when we start tinkering with geopolitics
- We still have to defend

Aramco Says Cyberattack Was Aimed at Production

By REUTERS
Published: December 9, 2012

JEDDAH, Saudi Arabia (Reuters) — Saudi Arabia’s national oil company, Aramco, said on Sunday that a cyberattack against it in August that damaged some 30,000 computers was aimed at stopping oil and gas production in Saudi Arabia, the biggest exporter in the Organization of the Petroleum Exporting Countries.

The attack on Saudi Aramco — which supplies a tenth of the world’s oil — failed to disrupt production, but was one of the most destructive hacker strikes against a single business.

“The main target in this attack was to stop the flow of oil and gas to local and international markets and thank God they were not able to achieve their goals,” Abdullah al-Saadon, Aramco’s vice president for corporate planning, said on Al Ekhbariya television. It was Aramco’s first comments on the apparent aim of the attack.

Hackers from a group called Cutting Sword of Justice claimed responsibility for the attack, saying that their motives were political and that the virus gave them access to documents from Aramco’s computers, which they threatened to release. No documents have yet been published.

Aramco and the Saudi Interior Ministry are investigating the attack. A ministry spokesman, Maj. Gen. Mansour al-Turki, said the attackers were an organized group operating from countries on four continents.

The attack used a computer virus known as Shamoon, which infected workstations on Aug. 15. The company shut its main internal network for more than a week. General Turki

FACEBOOK

TWITTER

GOOGLE+

SAVE

E-MAIL

SHARE

PRINT

REPRINTS

Fighting Back

When the APT comes through your backdoor. Unless you want some more, I think you better call ...



Source: Thomas Chopitea (@tomchop_)

How to Fight Back?

How to Fight Back?

- The days of thinking in purely IT terms are long gone

How to Fight Back?

- The days of thinking in purely IT terms are long gone
- Know your environment

How to Fight Back?

- The days of thinking in purely IT terms are long gone
- Know your environment
- Know your business

How to Fight Back?

- The days of thinking in purely IT terms are long gone
- Know your environment
- Know your business
- There's no such thing as an Anti-APT™
Silver Bullet

How to Fight Back?

- The days of thinking in purely IT terms are long gone
- Know your environment
- Know your business
- There's no such thing as an Anti-APT™
Silver Bullet



Easier said
than done

Security Awareness?

- Users click but do not think
- How to fight spear phishing attacks in an era with so many digital footprints?
- Think of RSA, Coca-Cola, State of South Carolina & so many others...
- Here is a \$1B question: how to measure effectiveness of security awareness?

Buy More Stuff™?

- Suuuuure... Be my guest. You've been stacking security stuff forever
- checkmarks for checklists
- Any measurable results?
- Do you even use correctly all the security stuff you have?

Do. It. Better

- Get a second look at your firewalls, DNS servers, system logs, DHCP logs, application logs and all the 'stuff' you already have
- Think. (re)Design. Log. Feed. Correlate. Alert

Best Practices?

- Put that in perspective
- Admittedly, risk assessment is hard to get right
- ... particularly if you don't know your business
- Ex.: how changing a password every 60 days help you?

The Inevitable AV Slide

The Inevitable AV Slide



SHA256: a82c2df6cf8c51db6332dc4f21575929d24b449af8f77085e940172b7fb6cfc8
File name: phut.exe
Detection ratio: 35 / 46
Analysis date: 2012-12-07 14:05:00 UTC (2 days, 23 hours ago)



More details

Analysis

Comments

Votes

Additional information

The Inevitable AV Slide

First seen by VirusTotal

2011-08-02 20:38:19 UTC (1 year, 4 months ago)

Last seen by VirusTotal

2012-12-07 14:05:00 UTC (2 days, 23 hours ago)

File names (max. 25)

1. B821684B0659109568BC078E387668004B2A4CD0.exe
2. jofuv.exe
3. phut.exe
4. fdbb0f0261eafa68e102fe4511d0e9c6

The Inevitable AV Slide

ByteHero	-	20121130
CAT-QuickHeal	-	20121207
ClamAV	-	20121207

The Inevitable AV Slide

ByteHero	-
CAT-QuickHeal	-
ClamAV	-

PCTools	-	20121207
Rising	-	20121207
Sophos	Troj/Tdss-HN	20121207
SUPERAntiSpyware	-	20121207
Symantec	WS.Reputation.1	20121207

The Inevitable AV Slide

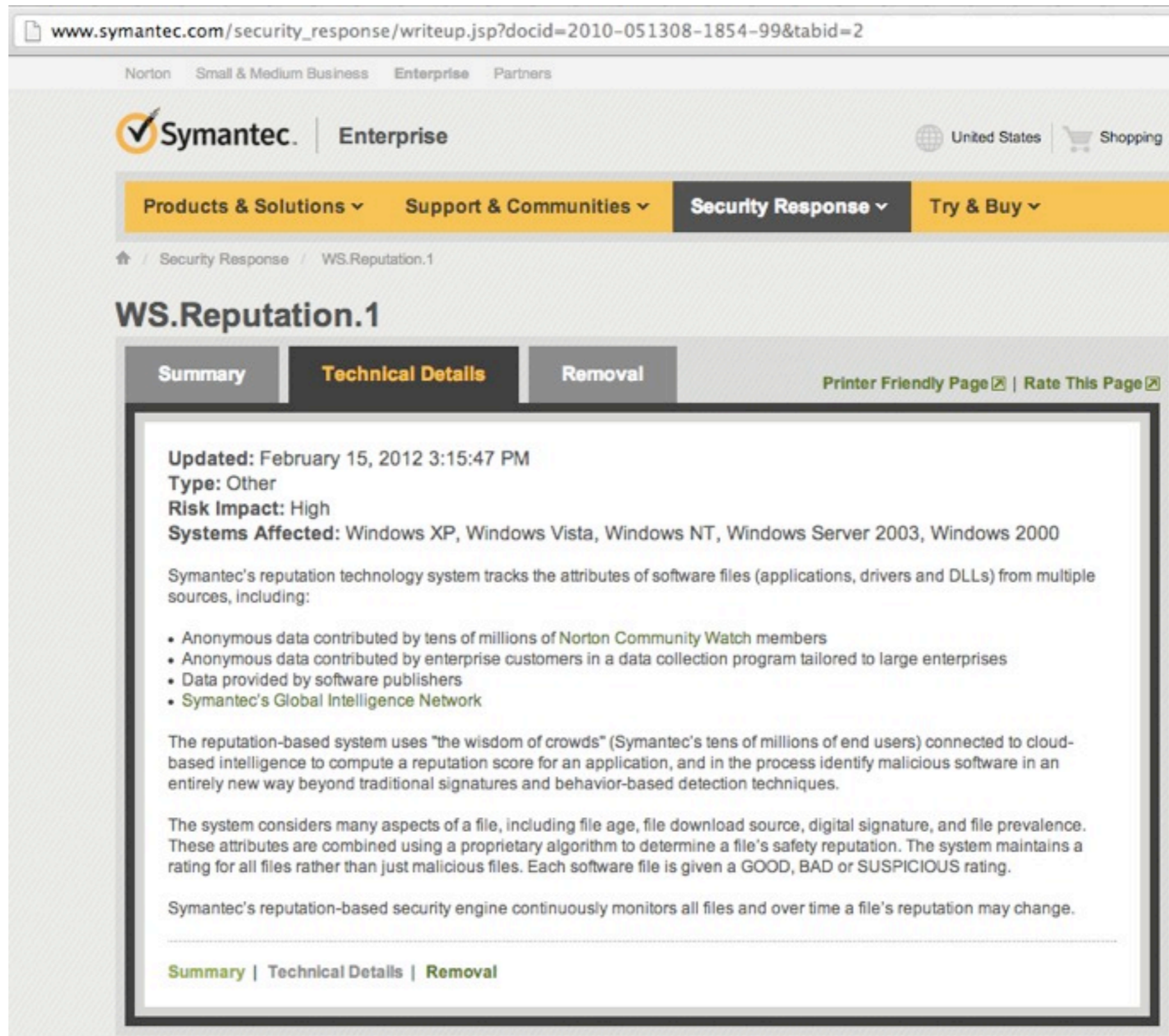
ByteHero	-
CAT-QuickHeal	-
ClamAV	-

PCTools	-	21207
Rising	-	21207
Sophos	Troj/Tdss-HN	21207
SUPERAntiSpyware	-	21207
Symantec	WS.Reputation.1	20121207

Specific Signature

Generic Signature

The Inevitable AV Slide



The screenshot shows a web browser window with the URL www.symantec.com/security_response/writeup.jsp?docid=2010-051308-1854-99&tabid=2. The page header includes the Symantec logo, the word "Enterprise", and navigation links for "Products & Solutions", "Support & Communities", "Security Response", and "Try & Buy". The main content area is titled "WS.Reputation.1" and has three tabs: "Summary", "Technical Details" (which is selected), and "Removal". There are also links for "Printer Friendly Page" and "Rate This Page".

Updated: February 15, 2012 3:15:47 PM
Type: Other
Risk Impact: High
Systems Affected: Windows XP, Windows Vista, Windows NT, Windows Server 2003, Windows 2000

Symantec's reputation technology system tracks the attributes of software files (applications, drivers and DLLs) from multiple sources, including:

- Anonymous data contributed by tens of millions of Norton Community Watch members
- Anonymous data contributed by enterprise customers in a data collection program tailored to large enterprises
- Data provided by software publishers
- Symantec's Global Intelligence Network

The reputation-based system uses "the wisdom of crowds" (Symantec's tens of millions of end users) connected to cloud-based intelligence to compute a reputation score for an application, and in the process identify malicious software in an entirely new way beyond traditional signatures and behavior-based detection techniques.

The system considers many aspects of a file, including file age, file download source, digital signature, and file prevalence. These attributes are combined using a proprietary algorithm to determine a file's safety reputation. The system maintains a rating for all files rather than just malicious files. Each software file is given a GOOD, BAD or SUSPICIOUS rating.

Symantec's reputation-based security engine continuously monitors all files and over time a file's reputation may change.

[Summary](#) | [Technical Details](#) | [Removal](#)

Another Example

Another Example



SHA256: abbbb994ced12cc151e138256724c17ef199c507e1ff9b91a147686feeb6d214

File name: Pnz.exe

Detection ratio: 40 / 46

Analysis date: 2012-12-07 10:27:09 UTC (3 days, 2 hours ago)


More details

Another Example

First seen by VirusTotal

2012-12-07 10:27:09 UTC (3 days, 2 hours ago)

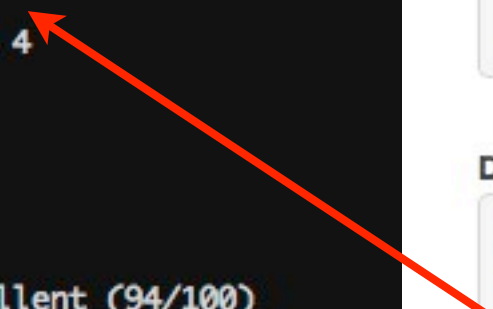
Last seen by VirusTotal

2012-12-07 10:27:09 UTC (3 days, 2 hours ago)

File names (max. 25)

1. Pnz.exe

```
Host: xe.com --> SUSPICIOUS
Associated DNS record(s): 4
- 216.220.38.25
- 216.220.38.20
- 216.220.38.23
- 216.220.38.24
MyWOT ratings:
- trustworthiness: excellent (94/100)
- confidence: 5/5 (73/100)
Geolocation:
- country: Canada (CAN)
- city: Toronto
- ASN number: AS12188
- ASN org: Q9 Networks Inc.
Matched source(s): 2/12
- PhishTank
- hpHosts
```



Registry activity

Set keys...

```
KEY: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\8DDYX0ZBPZ
TYPE: REG_SZ
VALUE: C:\abbbb994ced12cc151e138256724c17ef199c507e1ff9b91a147686feeb6d214.exe (successful)
```

Network activity

HTTP requests...

```
URL: http://newaitz.com/borders.php
TYPE: POST
UA: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)

URL: http://www.w3.org/TR/html4/loose.dtd
TYPE: GET
UA: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
```

DNS requests...

```
love21cn.com (59.151.18.18)
megaporn.com (107.21.243.42)
xe.com (216.220.38.23)
newaitz.com (141.8.226.2)
www.w3.org (128.30.52.37)
```

TCP connections...

```
141.8.226.2:80
128.30.52.37:80
```

Another Example









WS.Reputation.I???

Sophos	Mal/FakeAV-IZ	20121207
SUPERAntiSpyware	Trojan.Agent/Gen-Cryptic	20121207
Symantec	- ←	20121207
TheHacker	Trojan/Jorik.Skor.bou	20121207
TotalDefense	Win32/Renos.D!generic	20121206
TrendMicro	- ←	20121207

Japan's Space Agency Says Rocket Information Was Stolen by Computer Virus

By MARTIN FACKLER
Published: November 30, 2012

TOKYO — Japan's space agency said on Friday that information on one of its newest rockets was stolen from a desktop computer by someone using a computer virus.

-  FACEBOOK
-  TWITTER
-  GOOGLE+
-  SAVE
-  E-MAIL
-  SHARE
-  PRINT
-  REPRINTS

Connect With Us on Twitter
Follow
@nytimesworld for international breaking news and headlines.




Twitter List: Reporters and Editors

The Japan Aerospace Exploration Agency said that the virus in a computer at its Tsukuba Space Center northeast of Tokyo was found to be secretly collecting data and sending it outside the agency. The agency said that after the virus was detected by antivirus software on Nov. 21, it

conducted an emergency sweep for viruses that showed no other computers at the center had been infected.

The agency said it was unclear if the virus was a cyberattack. Japanese defense companies, however, have been recent targets of similar information-stealing viruses, some previously traced to China.

The data stolen from the space agency included information about the Epsilon, a solid-fuel rocket still under development. While the Epsilon is intended to launch satellite and space probes, solid-fuel rockets of that size can also have a military use as intercontinental ballistic missiles.

The Epsilon, whose first launching is scheduled for next autumn, will also feature new technology that will allow it to be remotely controlled by a personal computer. 

Invest in Skills?

- Yes, mere but **apt** mortals
- Build a CSIRT/CERT-like capability or hire a reputable, trustworthy one (who knows your env/business)
- Let them make sense of your security 'stuff' & bring it all together
- Leverage a toolset to fight back

YARA

Build your own AV (sort of)

What is YARA?

- Open Source Project created by Víctor Manuel Álvarez in 2008
- <https://code.google.com/p/yara-project/>
- multi-platform malware identification and classification tool
- Leverages rules

What is YARA?

- Open Source Project created by Víctor Manuel Álvarez in 2008
- <https://code.google.com/p/yara-project/>
- multi-platform malware identification and classification tool
- Leverages rules



We only care
about
detection

What is YARA?

```
usage: yara [OPTION]... [RULEFILE]... FILE | PID
options:
  -t <tag>          print rules tagged as <tag> and ignore the rest. Can be used more than once.
  -i <identifier>   print rules named <identifier> and ignore the rest. Can be used more than once.
  -n                print only not satisfied rules (negate).
  -g                print tags.
  -m                print metadata.
  -s                print matching strings.
  -l <number>       abort scanning after a <number> of rules matched.
  -d <identifier>=<value> define external variable.
  -r                recursively search directories.
  -f                fast matching mode.
  -v                show version information.

Report bugs to: <victor.alvarez@virustotal.com>
```

Or call `yara-python` from your own Python programs (look for `yara-ruby` if you worship gems)

YARA Rules

YARA Rules

- Set of strings, regular expressions and other binary patterns mixed with logic

YARA Rules

- Set of strings, regular expressions and other binary patterns mixed with logic
- Applicable to files or memory artifacts

YARA Rules

- Set of strings, regular expressions and other binary patterns mixed with logic
- Applicable to files or memory artifacts
- Fed to tools that will recursively scan files or analyze a memory image

YARA Rules

- Set of strings, regular expressions and other binary patterns mixed with logic
- Applicable to files or memory artifacts
- Fed to tools that will recursively scan files or analyze a memory image
- Rich, fully documented syntax

YARA Rules

Rules
= Signatures

- Set of strings, regular expressions and other binary patterns mixed with logic
- Applicable to files or memory artifacts
- Fed to tools that will recursively scan files or analyze a memory image
- Rich, fully documented syntax

Hello Rule!

```
1 rule embedded_executable
2
3   {
4     meta:
5       description = "Embedded executable detected"
6       author = "John Doe"
7       version = "v 1.0"
8       date = "2012.12.11"
9
10    strings:
11      $pattern = "This program cannot be run in DOS mode"
12
13    condition:
14      $pattern in (1024..filesize)
15
16  }
```

Hello Rule!

Rule name

```
1 rule embedded_executable
2
3 {
4     meta:
5         description = "Embedded executable detected"
6         author = "John Doe"
7         version = "v 1.0"
8         date = "2012.12.11"
9
10    strings:
11        $pattern = "This program cannot be run in DOS mode"
12
13    condition:
14        $pattern in (1024..filesize)
15
16 }
```

Hello Rule!

Rule name

Document
Your Rule

```
1 rule embedded_executable
2
3 {
4     meta:
5         description = "Embedded executable detected"
6         author = "John Doe"
7         version = "v 1.0"
8         date = "2012.12.11"
9
10    strings:
11        $pattern = "This program cannot be run in DOS mode"
12
13    condition:
14        $pattern in (1024..filesize)
15
16 }
```

Hello Rule!

Strings to
Look For

Rulename

Document
Your Rule

```
1 rule embedded_executable
2
3 {
4     meta:
5         description = "Embedded executable detected"
6         author = "John Doe"
7         version = "v 1.0"
8         date = "2012.12.11"
9
10    strings:
11        $pattern = "This program cannot be run in DOS mode"
12
13    condition:
14        $pattern in (1024..filesize)
15
16 }
```

Hello Rule!

Strings to
Look For

Rulename

Document
Your Rule

```
1 rule embedded_executable
2
3 {
4     meta:
5         description = "Embedded executable detected"
6         author = "John Doe"
7         version = "v 1.0"
8         date = "2012.12.11"
9
10    strings:
11        $pattern = "This program cannot be run in DOS mode"
12
13    condition:
14        $pattern in (1024..filesize)
15
16 }
```

How/Where?

Writing Rules

- BYOD (Bring Your Own Daktulos) ... or δακτυλος (finger in Greek)
- i.e. use the editor of your choice
- or try Yara Editor by Ivan Fontarensky
<https://code.google.com/p/yara-editor/>
- ...will hopefully mature fast enough :-)

String Searching

- Simple way to learn or guess at the functionality of a program
- Windows function names, error messages...
- Rather basic static analysis technique that can be automated using YARA
- Strings may be stored as ASCII or Unicode

DeleteCriticalSection
LeaveCriticalSection
EnterCriticalSection
InitializeCriticalSection
VirtualFree
VirtualAlloc
LocalFree
LocalAlloc
GetVersion
GetCurrentThreadId
GetThreadLocale
GetStartupInfoA
GetLocaleInfoA
GetCommandLineA
FreeLibrary
ExitProcess
WriteFile
UnhandledExceptionFilter
RtlUnwind
RaiseException
GetStdHandle
user32.dll
GetKeyboardType
MessageBoxA
advapi32.dll
RegQueryValueExA
RegOpenKeyExA
RegCloseKey
kernel32.dll
TlsSetValue
TlsGetValue
LocalAlloc
GetModuleHandleA
kernel32.dll
lstrcatW
SleepEx
FindResourceA
user32.dll
DestroyWindow
shell32.dll
ShellExecuteW
SHGetMalloc
SHGetDataFromIDListW
SHAddToRecentDocs
SHFileOperationW
comdlg32.dll
GetOpenFileNameA
0"0*020:0B0J0R0Z0b0j0r0z0
6S6b6
9\$9.989N9T9b9w9

Windows function
names & DLLs can
be looked up in
MSDN

Build a list of
'indicators' of
suspiciousness

ex. LoadLibrary,
GetProcAddress,
LdrLoadDll, ...

Libraries & Functions

The screenshot shows the Dependency Walker application for the file VodafoneMultimediaMessage.jpeg.ex_. The left pane displays a tree view of dependencies, including KERNEL32.DLL, USER32.DLL, ADVAPI32.DLL, MSVCRT.DLL, NTDLL.DLL, KERNELBASE.DLL, and various API-MS-WIN-SERVICE-*.DLL files. The right pane shows a list of exported functions from the selected module, with columns for PI, Ordinal, Hint, Function, and Entry Point. The function ControlService is highlighted.

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	0 (0x0000)	ChangeServiceConfig2A	0x02B254C2
C	N/A	1 (0x0001)	ChangeServiceConfigA	0x02B25254
C	N/A	2 (0x0002)	ControlService	0x02B24D5C
C	N/A	3 (0x0003)	ControlServiceExA	0x02B25CA0
C	N/A	4 (0x0004)	CreateServiceA	0x02B2567C
C	N/A	10 (0x000A)	I_ScRpcBindA	0x02B28E4E
C	N/A	11 (0x000B)	I_ScRpcBindW	0x02B28E3E
C	N/A	15 (0x000F)	NotifyServiceStatusChangeA	0x02B2A11D
C	N/A	16 (0x0010)	OpenSCManagerA	0x02B264F0
C	N/A	17 (0x0011)	OpenServiceA	0x02B27245
C	N/A	18 (0x0012)	QueryServiceConfig2A	0x02B26633

E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	0 (0x0000)	ChangeServiceConfig2A	0x00001086
C	2 (0x0002)	1 (0x0001)	ChangeServiceConfigA	0x0000105E
C	3 (0x0003)	2 (0x0002)	ControlService	0x00001086
C	4 (0x0004)	3 (0x0003)	ControlServiceExA	0x000010A0
C	5 (0x0005)	4 (0x0004)	CreateServiceA	0x00001068
C	6 (0x0006)	5 (0x0005)	I_QueryTagInformation	0x00001086
C	7 (0x0007)	6 (0x0006)	I_ScBroadcastServiceControlMessage	0x000010A0
C	8 (0x0008)	7 (0x0007)	I_ScIsSecurityProcess	0x00001090
C	9 (0x0009)	8 (0x0008)	I_ScPnPGetServiceName	0x00001086
C	10 (0x000A)	9 (0x0009)	I_ScQueryServiceConfig	0x00001086

Module | File Time Stamp | Link Time Stamp | File Size | Attr. | Link Checksum | Real Checksum | CPU | Subsystem

Libraries & Functions

msdn.microsoft.com/en-us/library/ms682108(v=vs.85).aspx

Home Library Learn Downloads Support Community Sign out | United States - English |

Search MSDN with Bing

- MSDN Library
- Windows Desktop App Development
- System Services
- Services
- Service Reference
- Service Functions
 - ChangeServiceConfig
 - ChangeServiceConfig2
 - CloseServiceHandle
 - ControlService**
 - ControlServiceEx
 - CreateService
 - DeleteService
 - EnumDependentServices
 - EnumServicesStatus
 - EnumServicesStatusEx
 - GetServiceDisplayName
 - GetServiceKeyName
 - Handler
 - HandlerEx
 - LockServiceDatabase
 - NotifyBootConfigStatus
 - NotifyServiceStatusChange
 - OpenSCManager
 - OpenService

ControlService function

6 out of 8 rated this helpful - [Rate this topic](#)

Sends a control code to a service.

To specify additional information when stopping a service, use the [ControlServiceEx](#) function.

Syntax

```
C++  
  
BOOL WINAPI ControlService(  
    _In_   SC_HANDLE hService,  
    _In_   DWORD dwControl,  
    _Out_  LPSERVICE_STATUS lpServiceStatus  
);
```

Parameters

hService [in]

A handle to the service. This handle is returned by the [OpenService](#) or [CreateService](#) function. The [access rights](#) required for this handle depend on the *dwControl* code requested.

dwControl [in]

This parameter can be one of the following control codes.

Packed Binaries

- Malware can be packed/obfuscated
- A packed binary is compressed & cannot be fully analyzed without decompressing it first
- Contains very few strings usually
- Highly limits static analysis

Packed Binaries

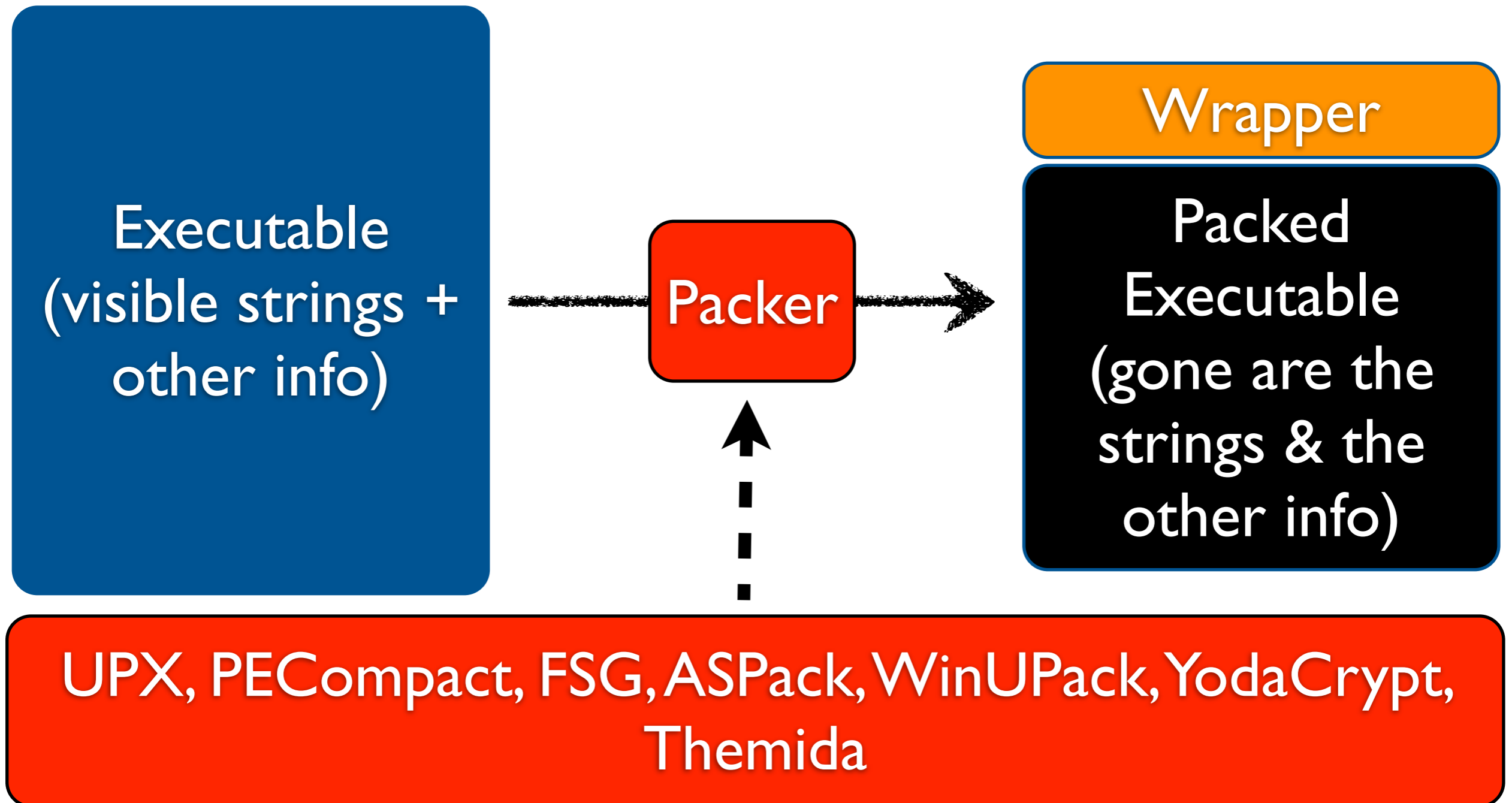
Packed Binaries

Executable
(visible strings +
other info)

Packer

UPX, PECompact, FSG, ASPack, WinUPack, YodaCrypt,
Themida

Packed Binaries



YARA vs. Packing

- Packed binaries is one sign of potential malware
- Wrapper program can be statically analyzed
- Use YARA rules to detect packers
- Build up on PeID rules
- Examples at <https://code.google.com/p/yara-project/wiki/PackerRules>

In Memory We Trust

- Once executed, packed binaries are decompressed
- Strings & other info are visible if you grab volatile memory
- Caution: malware may be able to detect your attempts at 'gaming' it in a VM & throw stub/fake artifacts at you

YARA & Volatility

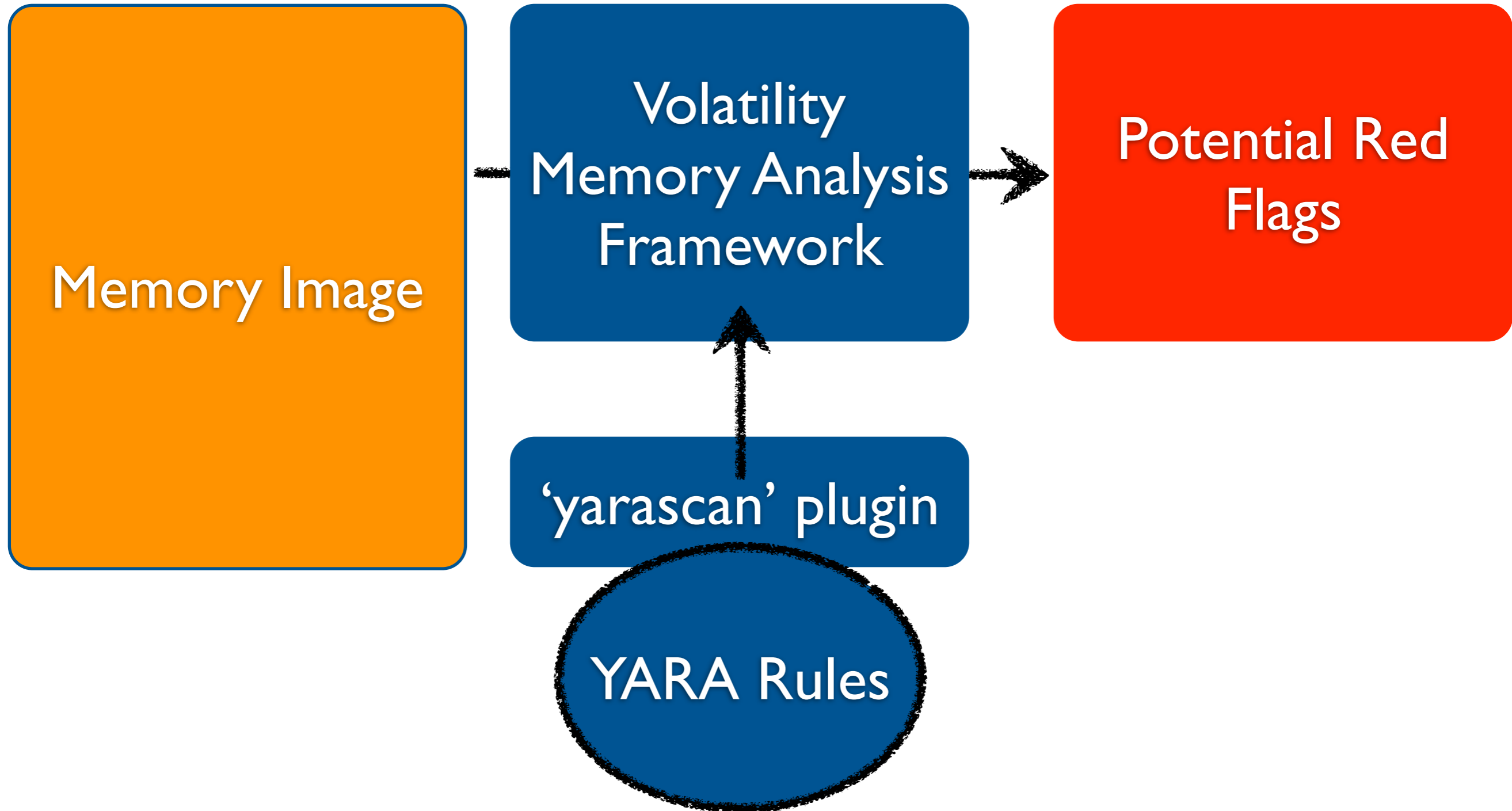
YARA & Volatility

A large orange rounded rectangle with a thin blue border, positioned on the left side of the slide.

Memory Image

YARA & Volatility

```
$ python vol.py -f mem.img yarascan --yara-file=/path/to/rules.yara
```



Use Cases

- Dissect RATs (Poison Ivy, Dark Comet, Ghost Rat, Extreme Rat...) & common utilities used by attackers
- Detect packed binaries, look for common passwords, bank domains, attempts at terminating AV services...
- Use in combination with Cuckoo sandbox, pehash, ssdeep, ...

IOC

Eye... Oh! See!
(To See, Drink Some Coffee)

What is IOC?

- A Mandiant initiative
- Indicator Of Compromise
- Collection of logically-grouped forensic artifacts from a wide array of sources
- registry, volatile memory, file system, binaries, application logs, firewall logs, hashes...

Compromise

- You don't build IOCs out of thin air
- Compromise leads to investigation leads to IOCs leads to better damage assessment leads to more IOCs leads to...
- You can also have IOCs handy to sweep your network & look for RATs & other shenanigans

OpenIOC

OpenIOC

<http://openioc.org/>

OpenIOC

<http://openioc.org/>

- Extensible XML Framework to construct & 'consume' IOCs

OpenIOC

<http://openioc.org/>

- Extensible XML Framework to construct & 'consume' IOCs
- Released in 2011 by Mandiant, no strings attached

OpenIOC

<http://openioc.org/>

- Extensible XML Framework to construct & 'consume' IOCs
- Released in 2011 by Mandiant, no strings attached
- Field tested, backed by real-world experience

OpenIOC

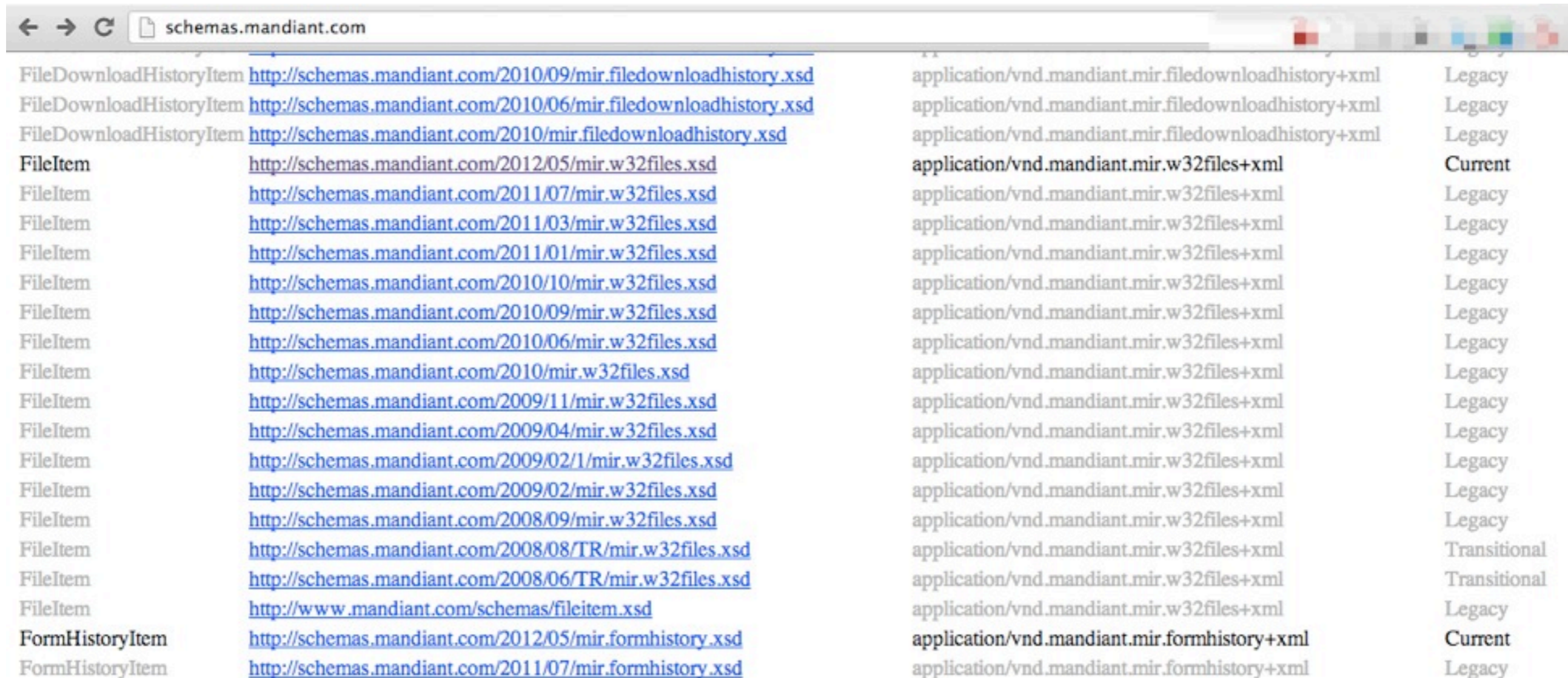
<http://openioc.org/>

- Extensible XML Framework to construct & 'consume' IOCs
- Released in 2011 by Mandiant, no strings attached
- Field tested, backed by real-world experience
- Extensively used in Mandiant Intelligent Response (commercial solution)

XML Schemas

- XML Schemas are at the heart of OpenIOC
- Available at <http://schemas.mandiant.com>
- Each OpenIOC schema defines a namespace
- A namespace is a set of items (or terms) related to a given artifact group

XML Schemas



Schema Name	URL	Namespace	Status
FileDownloadHistoryItem	http://schemas.mandiant.com/2010/09/mir.filedownloadhistory.xsd	application/vnd.mandiant.mir.filedownloadhistory+xml	Legacy
FileDownloadHistoryItem	http://schemas.mandiant.com/2010/06/mir.filedownloadhistory.xsd	application/vnd.mandiant.mir.filedownloadhistory+xml	Legacy
FileDownloadHistoryItem	http://schemas.mandiant.com/2010/mir.filedownloadhistory.xsd	application/vnd.mandiant.mir.filedownloadhistory+xml	Legacy
FormItem	http://schemas.mandiant.com/2012/05/mir.w32files.xsd	application/vnd.mandiant.mir.w32files+xml	Current
FormItem	http://schemas.mandiant.com/2011/07/mir.w32files.xsd	application/vnd.mandiant.mir.w32files+xml	Legacy
FormItem	http://schemas.mandiant.com/2011/03/mir.w32files.xsd	application/vnd.mandiant.mir.w32files+xml	Legacy
FormItem	http://schemas.mandiant.com/2011/01/mir.w32files.xsd	application/vnd.mandiant.mir.w32files+xml	Legacy
FormItem	http://schemas.mandiant.com/2010/10/mir.w32files.xsd	application/vnd.mandiant.mir.w32files+xml	Legacy
FormItem	http://schemas.mandiant.com/2010/09/mir.w32files.xsd	application/vnd.mandiant.mir.w32files+xml	Legacy
FormItem	http://schemas.mandiant.com/2010/06/mir.w32files.xsd	application/vnd.mandiant.mir.w32files+xml	Legacy
FormItem	http://schemas.mandiant.com/2010/mir.w32files.xsd	application/vnd.mandiant.mir.w32files+xml	Legacy
FormItem	http://schemas.mandiant.com/2009/11/mir.w32files.xsd	application/vnd.mandiant.mir.w32files+xml	Legacy
FormItem	http://schemas.mandiant.com/2009/04/mir.w32files.xsd	application/vnd.mandiant.mir.w32files+xml	Legacy
FormItem	http://schemas.mandiant.com/2009/02/1/mir.w32files.xsd	application/vnd.mandiant.mir.w32files+xml	Legacy
FormItem	http://schemas.mandiant.com/2009/02/mir.w32files.xsd	application/vnd.mandiant.mir.w32files+xml	Legacy
FormItem	http://schemas.mandiant.com/2008/09/mir.w32files.xsd	application/vnd.mandiant.mir.w32files+xml	Legacy
FormItem	http://schemas.mandiant.com/2008/08/TR/mir.w32files.xsd	application/vnd.mandiant.mir.w32files+xml	Transitional
FormItem	http://schemas.mandiant.com/2008/06/TR/mir.w32files.xsd	application/vnd.mandiant.mir.w32files+xml	Transitional
FormItem	http://www.mandiant.com/schemas/fileitem.xsd	application/vnd.mandiant.mir.w32files+xml	Legacy
FormHistoryItem	http://schemas.mandiant.com/2012/05/mir.formhistory.xsd	application/vnd.mandiant.mir.formhistory+xml	Current
FormHistoryItem	http://schemas.mandiant.com/2011/07/mir.formhistory.xsd	application/vnd.mandiant.mir.formhistory+xml	Legacy

```

1 <?xml version="1.0" encoding="utf-8"?>
2 <xs:schema elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
3   <xs:element name="FileItem" nillable="true" type="FileItem" />
4   <xs:complexType name="FileItem">
5     <xs:complexContent mixed="false">
6       <xs:extension base="HashItem">
7         <xs:sequence>
8           <xs:element minOccurs="0" maxOccurs="1" name="DevicePath" type="xs:string" />
9           <xs:element minOccurs="0" maxOccurs="1" name="FullPath" type="xs:string" />
10          <xs:element minOccurs="0" maxOccurs="1" name="Drive" type="xs:string" />
11          <xs:element minOccurs="0" maxOccurs="1" name="FilePath" type="xs:string" />
12          <xs:element minOccurs="0" maxOccurs="1" name="FileName" type="xs:string" />
13          <xs:element minOccurs="0" maxOccurs="1" name="FileExtension" type="xs:string" />
14          <xs:element minOccurs="1" maxOccurs="1" name="SizeInBytes" nillable="true" type="xs:long" />
15          <xs:element minOccurs="1" maxOccurs="1" name="Created" nillable="true" type="xs:dateTime" />
16          <xs:element minOccurs="1" maxOccurs="1" name="Modified" nillable="true" type="xs:dateTime" />
17          <xs:element minOccurs="1" maxOccurs="1" name="Accessed" nillable="true" type="xs:dateTime" />
18          <xs:element minOccurs="1" maxOccurs="1" name="Changed" nillable="true" type="xs:dateTime" />
19          <xs:element minOccurs="1" maxOccurs="1" name="FilenameCreated" nillable="true" type="xs:dateTime" />
20          <xs:element minOccurs="1" maxOccurs="1" name="FilenameModified" nillable="true" type="xs:dateTime" />
21          <xs:element minOccurs="1" maxOccurs="1" name="FilenameAccessed" nillable="true" type="xs:dateTime" />
22          <xs:element minOccurs="1" maxOccurs="1" name="FilenameChanged" nillable="true" type="xs:dateTime" />
23          <xs:element minOccurs="1" maxOccurs="1" name="FileAttributes" nillable="true" type="FileAttributes" />
24          <xs:element minOccurs="0" maxOccurs="1" name="Username" type="xs:string" />
25          <xs:element minOccurs="0" maxOccurs="1" name="SecurityID" type="xs:string" />
26          <xs:element minOccurs="1" maxOccurs="1" name="SecurityType" nillable="true" type="SIDTypes" />
27          <xs:element minOccurs="1" maxOccurs="1" name="INode" nillable="true" type="xs:unsignedLong" />
28          <xs:element minOccurs="0" maxOccurs="1" name="StreamList" type="ArrayOfStreamItem" />
29          <xs:element minOccurs="0" maxOccurs="1" name="PEInfo" type="PEInfo" />
30          <xs:element minOccurs="1" maxOccurs="1" name="PeakEntropy" type="xs:double" />
31          <xs:element minOccurs="1" maxOccurs="1" name="PeakCodeEntropy" type="xs:double" />
32          <xs:element minOccurs="0" maxOccurs="1" name="StringList" type="ArrayOfString" />
33        </xs:sequence>
34      </xs:extension>
35    </xs:complexContent>
36  </xs:complexType>
37  <xs:complexType name="HashItem">
38    <xs:complexContent mixed="false">
39      <xs:extension base="ItemBase">
40        <xs:sequence>
41          <xs:element minOccurs="0" maxOccurs="1" name="Md5sum" type="Md5HashSum" />
42          <xs:element minOccurs="0" maxOccurs="1" name="Sha1sum" type="Sha1HashSum" />
43          <xs:element minOccurs="0" maxOccurs="1" name="Sha256sum" type="Sha256HashSum" />
44        </xs:sequence>
45      </xs:extension>
46    </xs:complexContent>
47  </xs:complexType>

```


Let's Delve Into a Term

```
<xs:complexType name="PEInfo">
  <xs:sequence>
    <xs:element minOccurs="1" maxOccurs="1" name="Type" type="PEType" />
    <xs:element minOccurs="1" maxOccurs="1" name="Subsystem" nillable="true" type="SubsystemType" />
    <xs:element minOccurs="1" maxOccurs="1" name="BaseAddress" nillable="true" type="xs:unsignedLong" />
    <xs:element minOccurs="1" maxOccurs="1" name="PETimeStamp" nillable="true" type="xs:dateTime" />
    <xs:element minOccurs="0" maxOccurs="1" name="PEChecksum" type="PEChecksumInfo" />
    <xs:element minOccurs="1" maxOccurs="1" name="ExtraneousBytes" nillable="true" type="xs:int" />
    <xs:element minOccurs="0" maxOccurs="1" name="Exports" type="ExportInfo" />
    <xs:element minOccurs="0" maxOccurs="1" name="EpJumpCodes" type="EPJumpCodeInfo" />
    <xs:element minOccurs="0" maxOccurs="1" name="DetectedAnomalies" type="ArrayOfString" />
    <xs:element minOccurs="0" maxOccurs="1" name="DigitalSignature" type="DigitalSignatureInfo" />
    <xs:element minOccurs="0" maxOccurs="unbounded" name="DetectedEntryPointSignature" type="EntryPointSignature" />
    <xs:element minOccurs="0" maxOccurs="1" name="Sections" type="SectionsInfo" />
    <xs:element minOccurs="0" maxOccurs="1" name="VersionInfoList" type="ArrayOfVersionInfoItem" />
    <xs:element minOccurs="0" maxOccurs="1" name="ResourceInfoList" type="ArrayOfResourceInfoItem" />
    <xs:element minOccurs="0" maxOccurs="1" name="ImportedModules" type="ArrayOfModule" />
  </xs:sequence>
</xs:complexType>
```

Houston, we've got a problem

- There are hundreds of OpenIOC terms
- While most have explicit names, there is no detailed documentation for the meaning of each term
- Read the schema Luke!

Houston, please reply...

- OpenIOC doesn't tell you how to search or retrieve terms
- It's up to tools built on top of OpenIOC to implement what they need to dig artifacts out

Tools

- Mandiant provides two free tools for Microsoft Windows platforms
- IOC Editor to write & compare IOCs
- IOC Finder to 'consume' IOCs
- Redline, Mandiant's free memory & file investigation tool can also 'consume' IOCs

Tools

The screenshot shows a software window titled "Start your Analysis Session". It is divided into two main sections: "Instructions" and "Configuration".

Instructions:

Select the location of your audit data folder produced by your data collector. Redline will analyze this data to aid in navigation and to assist in the identification of potential issues. Redline can also search for Indicators of Compromise (described below) at this time. If you wish to search for Indicators of Compromise (IOCs) at a later time, this option can be found under the IOC reports tab.

Indicators of Compromise:

Indicators of Compromise are forensic artifacts left behind by an intrusion. An IOC file describes these artifacts using the OpenIOC format. When configuring an audit, Redline verifies that the correct data exists, or will be acquired, so that these artifacts can be identified.

Note that IOC sets may be run against an audit after collection and analysis. Redline will issue a warning if an IOC is selected which requires data that was not collected in the original audit.

Configuration:

Audit Location: [Open Folder](#)
Choose a directory containing the Audit for Redline to Analyze

Indicators of Compromise Location: [Open Folder](#)
Choose a directory containing your Indicators of Compromise

IOC Editor

The screenshot shows the IOC Editor application window. The title bar reads "IOCe 2.1.100". The menu bar includes "File", "Search", "Options", and "Help".

Item List:

Name	Created	Updated	S
ZEUS ANALYTICDNS.COM (BACKDOOR)	06/03/2012 01:22:52	13/10/2012 07:17:14	L

A red arrow points to the "Updated" column of the first row.

Item Details:

- Name: ZEUS ANALYTICDNS.COM (BACKDOOR)
- Author: LucasEratus
- GUID: 10ccb93f-970b-4f0a-8e0c-5772cdd9f...
- Description: This malware is a variant of the Zeus Bot. Change the exe size range to make it fuzzy and detect exe files in the directory it gets dropped to (e.g. 100000 TO 200000). That will allow it to catch all versions and variants that still copy to that location.

Definition:

Definition: DnsEntryItem/Host contains analyticdns.com

- File PEInfo VersionInfoList VersionInfo OriginalFilename is Y2gtqjxmvoynnm.exe
- File CertificateSubject is Tfrbpcz
- File PEInfo VersionInfoList VersionInfo CompanyName is Walter Hintenaus
- File PEInfo VersionInfoList VersionInfo InternalName is Lodge Tuna Angel
- File PEInfo VersionInfoList VersionInfo ProductName is Loyal
- File PEInfo VersionInfoList VersionInfo FileDescription is Seth Achoo Xiv
- Process Handle Name contains -DED2-FBD9A76483EE}
- Process Handle Name contains -6CED-298D15DD61B5}
- Process Handle Name contains -2E3B-B788507ACFBF}
- Process Handle Name contains -377E-962C6878EE14}

AND

- OR
 - AND
 - File Extension is exe
 - OR
 - File Size is [100000 TO 200000]
 - File Compile Time is 2011-07-24T05:58:28Z
 - AND
 - File Extension is tmp
 - File Size is 0
- OR
 - AND
 - File Full Path contains \Users\
 - File Full Path contains \AppData\Roaming\
 - AND
 - File Full Path contains \Application Data\
 - File Full Path contains Documents
 - File Full Path contains Settings

A red arrow points to the "File Size is [100000 TO 200000]" entry in the definition.

Buttons: Delete, Save

IOC Editor

The screenshot displays the IOC Editor interface. On the left, a search query tree is visible, starting with an AND operator, followed by an OR operator, and then several nested AND and OR operators. The tree includes conditions such as "File PEInfo VersionIn", "Process Handle Name c", "File Extension", "File Size", "File Comp", "File Full Pat", and "File Size is".

In the center, a menu is open, showing options: "Add Item", "Add Logic", and "Change Logic". Below these, a list of item types is displayed, with "EventLogItem" selected. The list includes: Favorites, CookieHistoryItem, Email, EventLogItem, FileDownloadHistoryItem, FileItem, FormHistoryItem, HiveItem, HookItem, ModuleItem, Network, PortItem, ProcessItem, RegistryItem, ServiceItem, Snort, SystemInfoItem, TaskItem, UrlHistoryItem, UserItem, and VolumeItem.

On the right, a list of event log items is shown, including: EventLog blob, EventLog category, EventLog categoryNum, EventLog CorrelationActivityId, EventLog CorrelationRelatedActivityId, EventLog ExecutionProcessId, EventLog ExecutionThreadId, EventLog GenTime, EventLog ID, EventLog index, EventLog log, EventLog machine, EventLog Message, EventLog reserved, EventLog source, EventLog type, EventLog unformattedMessage, EventLog user, and EventLog writeTime.

At the top right, a text field contains the search query: "Filename is Y2gtqjxmvounynm.exe".

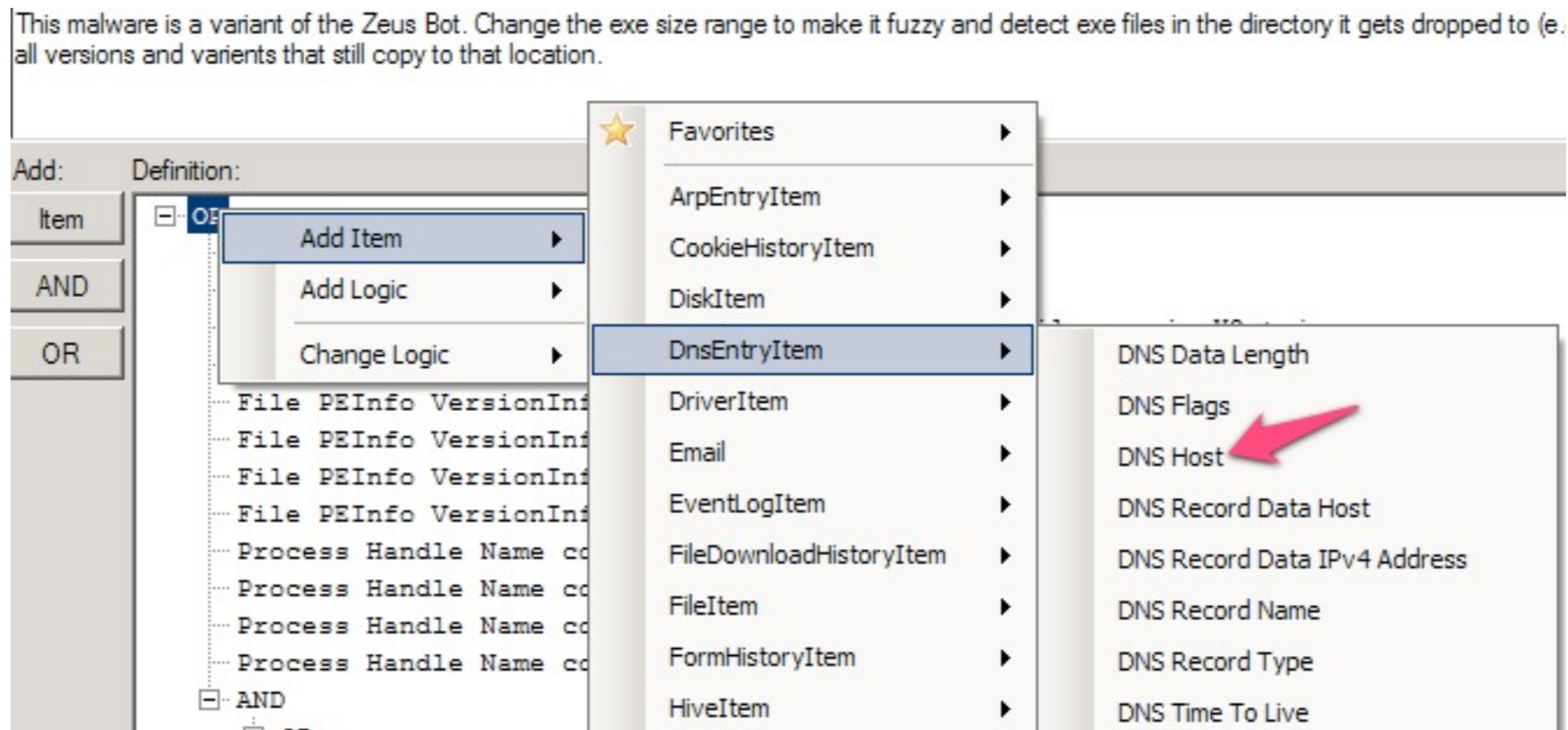
IOC Editor

Some namespaces (or categories) such as `DnsEntryTerm` are not available by default

IOC Editor

Some namespaces (or categories) such as DnsEntryTerm are not available by default

Get them from <http://openioc.org/terms/IOCFinder.iocterms> & drop into 'C:\Program Files (x86)\Mandiant\Mandiant IOCe'



Authored By:

@LucasErratus

Description:

This malware is a variant of the Zeus Bot. Change the exe size range to make it fuzzy and detect exe files in the directory it gets dropped to (e.g. 100000 TO 200000). That will allow it to catch all versions and variants that still copy to that location.

Indicators:

OR

DnsEntryItem/Host contains myapp-ups.com

DnsEntryItem/Host contains analyticdns.com

File PEInfo VersionInfoList VersionInfo OriginalFilename is Y2gtqjxmvounynm.exe

File CertificateSubject is Tfrbpcs

File PEInfo VersionInfoList VersionInfo Companyname is Walter Hintenaus

File PEInfo VersionInfoList VersionInfo InternalName is Lodge Tuna Angel

File PEInfo VersionInfoList VersionInfo ProductName is Loyal

File PEInfo VersionInfoList VersionInfo FileDescription is Seth Achoo Xiv

Process Handle Name contains -DED2-FBD9A76483EE}

Process Handle Name contains -6CED-298D15DD51B5}

Process Handle Name contains -2E3B-B788507ACFBF}

Process Handle Name contains -377E-962C6878EE14}

AND

OR

AND

File Extension is exe

OR

File Size is [154192 TO 154192]

File Compile Time is 2011-07-24T05:58:28Z

AND

File Extension is tmp

File Size is 0

OR

AND

File Full Path contains \Users\

File Full Path contains \AppData\Roaming\

AND

File Full path contains \Application Data\

File Full path contains Documents

File Full path contains Settings

Download:

[10ccb93f-970b-4f0a-8e0c-5772cdd90a20.ioc](#)

Indicators:

OR

DnsEntryItem/Host contains myapp-ups.com

DnsEntryItem/Host contains analyticdns.com

File PEInfo VersionInfoList VersionInfo OriginalFilename is Y2gtqjxmvounynm.exe

File CertificateSubject is Tfrbpcs

File PEInfo VersionInfoList VersionInfo Companyname is Walter Hintenaus

File PEInfo VersionInfoList VersionInfo InternalName is Lodge Tuna Angel

File PEInfo VersionInfoList VersionInfo ProductName is Loyal

File PEInfo VersionInfoList VersionInfo FileDescription is Seth Achoo Xiv

Process Handle Name contains -DED2-FBD9A76483EE}

Process Handle Name contains -6CED-298D15DD51B5}

Process Handle Name contains -2E3B-B788507ACFBF}

Process Handle Name contains -377E-962C6878EE14}

AND

OR

AND

File Extension is exe

OR

File Size is [154192 TO 154192]

File Compile Time is 2011-07-24T05:58:28Z

AND

File Extension is tmp

File Size is 0

OR

AND

File Full Path contains \Users\

File Full Path contains \AppData\Roaming\

AND

File Full path contains \Application Data\

File Full path contains Documents

File Full path contains Settings

IOC Finder

- CLI tool
- Two stages
- Collect forensic evidence from target(s) of interest
- Generate a report on the analyst's machine

IOC Finder

```
C:\Users\Saad Kadhi>mandiant_ioc_finder.exe collect -h
[...]

-----
mandiant_ioc_finder collect options:
-----

-o output_dir
    Output directory for data collection from the host lstrip is
    run on. Defaults to current working directory.
-d drive
    Drive letter to execute data collection on, e.g. c:. You can pass this
    flag in more than once. Defaults to %SystemDrive%.
[...]
```

```
C:\Users\Saad Kadhi>mandiant_ioc_finder.exe report -h
[...]

-----
mandiant_ioc_finder report options:
-----

-i input_iocs
    Name of an ioc file, zipfile or directory
    containing one or more .ioc files formatted in OpenIOC 1.0
    or greater. Multiple -i flags may be specified for multiple
    sources.
-s source_data
    Path to a directory containing one or more data collections
    to process for IOC hit reporting. mandiant_ioc_finder expects the
    directory structure to conform to the MIR Agent local data
    collection layout standard.
-t html|doc
    Specifies report type - either HTML or MS Word XML.
-o output_file (doc)|output folder (html)
    For the HTML format (-t html), this is the directory the report is
    generated in. Defaults to ./report/YYYYMMDDhhmmss.
    - NOTE: Currently Firefox is the only supported browser.
[...]
```

pyioc

<https://github.com/jeffbryner/pyioc>

- Set of Python tools to check IOCs against targets of interest
- Written by Jeff Bryner & released under a GPL v3 license
- Agent-server model. Agents connect to server through SSL/SOAP, get IOCs, perform checks and send back the results

A Few pyioc Issues

- Why do you think IOC Finder works in two stages?
- Hint: are the IOCs ever present on the targets of interest?
- Only 18 supported terms belonging to the FileItem, PortItem, ProcessItem & RegistryItem categories
- Still, pyioc is a laudable effort that must be supported

Closing Thoughts

Excited about IOC & YARA?
Well... not so fast

Sharing

- Sharing of IOCs & YARA rules is quite (if not very) rare
- Investment needed to build them
- Competitive edge they give you in the battle against malware and miscellaneous threat actors (treasure trove)
- & you don't want to be giving away intel to the attackers

Time + Budget = Plan

- You don't want to dissect every malware variant out there and get overburned
- First, build IOCs & YARA rules to detect RATs and common utilities used by attackers once they gain a foothold on your network
- Then move to persistence, logs and other telltale signs of mischief



45 rue de la chaussée d'Antin
75009 Paris
FRANCE

Tél. : +33 (0)1 53 16 30 60 - Fax : +33 (0)1 53 16 30 62
contact@hapsis.fr



This work is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License