

Real World Attacks in Action

Erik Yunghans, Consulting Engineer



SSN Data

Online
6

Register
25

Total
5138

Scans
1651

SSN
2822339

SSH
780

Paypal
28132

Credit cards
655533

Balance
\$0

Shop

SSN

Filter +

SSN: 2822339

Add money

#	Seller	First name	Middle name	Last name	Street address	Home phone	City	State	Zip code	Year of birth	Cost	Action
380	admin	Andy	J	Leiker	7338 Kenton	XXX-XXX-0006	Shawnee	KS	66227	1976	\$1.40	BUY
506	admin	Jonathan	Duran	Noel	506 N Henry St Upper APT	XXX-XXX-9511	Bay City	MI	48706	1985	\$1.40	BUY
520	admin	Marquesa	Nicole	Colwell	264 Greenway Drive	XXX-XXX-4117	Scottsburg	IN	47170	1983	\$1.40	BUY
523	admin	BRENDA	MARCELL	GRUBBS	10600 MARS HILL ROAD	XXX-XXX-6868	BAUXITE	AR	72011	1948	\$1.40	BUY
534	admin	john	e	reese	2517 old congo rd	XXX-XXX-4377	Benton	AR	72019	1979	\$1.40	BUY
563	admin	Jeffery	Alan	Bustamante	3378 Burton Chapel Rd	XXX-XXX-9186	Yanceyville	NC	27379	1973	\$1.40	BUY
574	admin	eric	eugene	rhymer	9225 styers ferry rd	XXX-XXX-1980	Clemmons	NC	27012	1983	\$1.40	BUY



Understand the Intent

- Malware has a ultimate **'business purpose'**
- Functionality is **specific** to that purpose
- **Co-infection** is the norm, not the exception
 - Purpose may shift when target is acquired
- Functionality can be extended
 - Exfiltration
 - Command & Control
 - Post-Operation
- Attackers understand defense strategy
 - Circumvention is trivial

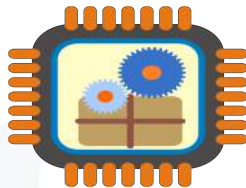


Circumventing Traditional Security Controls

- Attackers understand technical/organizational capabilities and defense tactics
- Circumvention of traditional controls is **automated**
 - Replace/substitute when detected
 - Daily campaigns with differing attributes
- Most organizations **do not** properly handle, classify or understand what they encounter
 - Rely solely on one isolated technology
 - Wrongly assume that removal is enough



Firewall



IPS



URL Filtering/Proxy



Endpoint Security

Commodity Malware: SaaS

- Reseller Model
 - No direct interaction with creator
- Purchase through trusted 3rd party escrow
 - BitCoin, WebMoney, Ukash, Skrill, Perfect Money
- Hosted or delivered (Binary & Backend)
 - Commercial Software Protection
 - ionCube PHP Encoder used to domain/time lock
 - Hard-coded backend location
 - Change of backend requires new binary + cost
- Modules, add-on's, custom development
 - Scaled pricing
 - Example: DDoS module




Ransomware: SaaS Advertisement

Private software SyndicateS sale:

- **WinLocker** – software to lock Windows OS (US, EU, can work without admin rights). 1500\$ (build) rebuild free
- **CryptoLocker** – software for file encryption in Windows OS. 2000\$ (build) rebuild free
- **Dropper DLL** – run DLL in memory. 1500\$ (build) rebuild 50\$
- **Non-resident Loader without admin rights.** Run up to 3 files. Size is about 7 KB. 1000\$ builder
- **Customization is available.** Optionally builders are sold upon agreement. Source code as well. All details in Jabber.

RIG Exploit Kit: SaaS Example

 **RIG exploit kit \$50 Day | \$200 Week | \$700 Month**
« on: February 07, 2015, 07:32:58 PM »

Are pleased to introduce you to RIG exploits v2.0

- Work On all WinOS 32 / 64bi
- Bypass UAC on exploits
- Fast cleaning + cleaning on request
- Keep Large volumes of traffic, no traffic limits
- We provide always clean and trust domains with automatic check on the blacklist
- We use CVE-2013-7331 for detect and stop AV or virtual machines.
- API with automatic delivery

Each account has a 2 stream and can ship 2 different exe

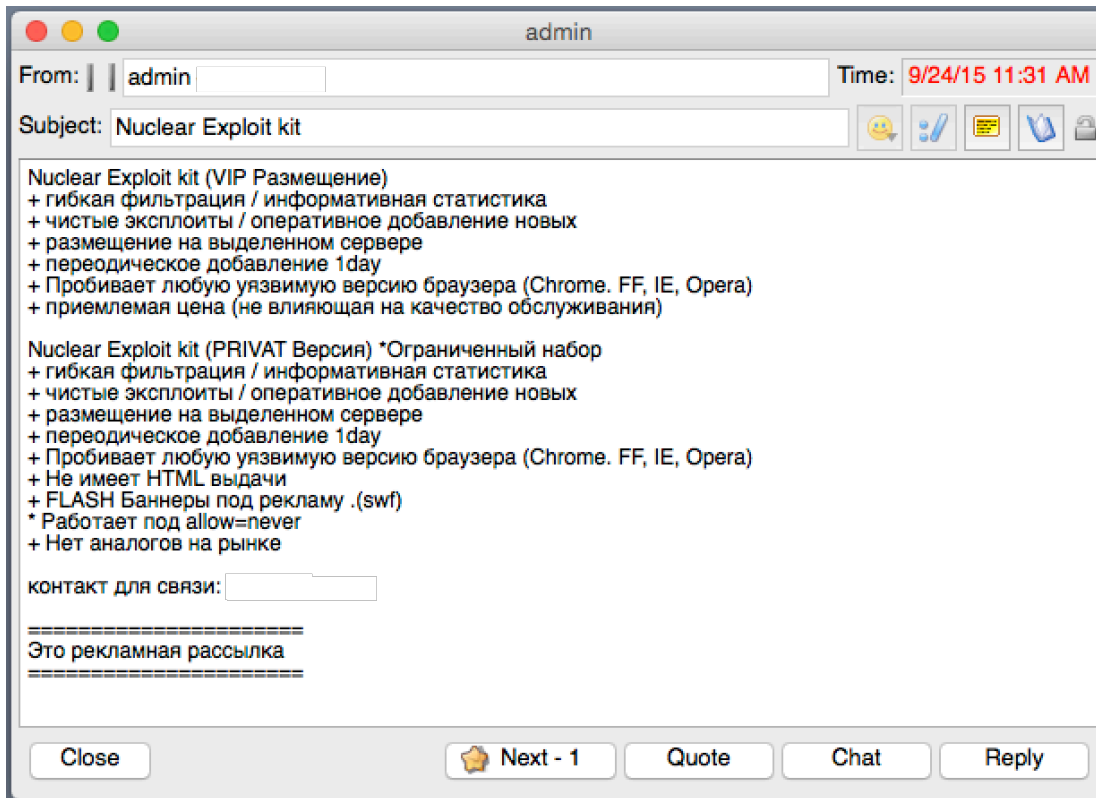
Current exploits:

- ✓ **Java:** CVE-2012-0507
- ✓ **Java:** CVE-2013-2465
- ✓ **IE7-8-9:** CVE-2013-2551
- ✓ **IE10:** CVE-2013-0322
- ✓ **Flash:** CVE-2014-0497
- ✓ **Flash:** CVE-2015-0311
- ✓ **Silverlight:** CVE-2013-0074

An average rate of 10-20%

- Reseller Model
- Proxy architecture
- Landing page redirects into exploit core
- 2 EXE's per flow
- CVE-2013-7331 XMLDOM ActiveX Control Vulnerability leveraged to enumerate all installed Antivirus software
- RIG iterates over installed plug-ins and versions to find appropriate exploit
- 10-20% advertised effective rate per hit

Nuclear Exploit Kit



Nuclear Exploit kit (VIP accommodation)

- + Flexible filtering / informative statistics
- + Net exploits / rapid addition of new
- + Accommodation on a dedicated server
- + Periodically adding 1day
- Punches + any vulnerable version of the browser (Chrome, FF, IE, Opera)
- + Reasonable price (does not affect the quality of service)

Nuclear Exploit kit (PRIVAT version) *

- Limited set
- + Flexible filtering / informative statistics
- + New exploits / rapid addition of new
- + Accommodation on a dedicated server
- + Periodically adding 1day
- Punches + any vulnerable version of the browser (Chrome, FF, IE, Opera)
- + Has an HTML extradition
- + FLASH Banners for advertising. (Swf)
- * Works under the allow = never
- + There are no analogues on the market

CTB-Locker Affiliate Panel

- Price Rules
- Payouts
- Statistics
- Installs
- Support
- API

CTB-Locker affiliate server. 08:11:25

Home Price rules Payouts Stats Installs Get EXE Support User messages API

Registered since: 25 Oct 2014

Total installs: 1653

Keys paid: 6

Total payouts: 2.45032303 BTC

Your domains are:
q4vyrzddq25a4jhf.onion PRIMARY ACTIVE
gvgfgt5dibj67dsg.onion PRIMARY GATE ACTIVE

Primary domains are built into exe.
Active domains are handled by TOR and accessible.
Gate domains are mirrors for gate usage, hidden from user to lower abuses.

03.02.2015: v2.12 added Franch translation, many fixes against AV

27.01.2015: v2.11 added Spanish and Latvian translations, some minor updates.

15.01.2015: added mirror administrative domain to avoid broken circuits: **ctb2ndyexrfj7zsn.onion**

14.01.2015: v2.10 Minor protocol updates

12.01.2015: v2.9 Many updates to installation and reporting functions. Added mirror domains to avoid ban under gates. Added German translation.

25.12.2014: v2.8 minor fixes for gui under system priveleges

24.12.2014: v2.7 Many changes to increase installation rate at different OS configurations. GUI changed to reduce exe size.

16.12.2014: v2.6 VM detection fixes, some minor changes to decrease report lag, minor changes for server OS

15.12.2014: v2.5 Added Dutch and Italian translations.

24.11.2014: v2.4 Minor locker and server interface changes

14.11.2014: v2.3 fixed compatibility with Windows 8 and Windows 10. Added stats counters.

26.10.2014: Minor updates to v2.2

14.10.2014: v2.1 Fixed issue on x64 systems

10.10.2014: Update 2.0. Major update, impooved anti-heuristic, changed installation and encryption scheme, added total files size to the rules. You can

paloalto NETWORKS

CTB-Locker Affiliate: Price Rules

CTB-Locker affiliate server. 08:20:25

Home Price rules Payouts Stats Installs Get EXE Support User messages API

No rules defined

Country code in list: * and SubID=* and Size>0 Mb or files => Price:

Comment:

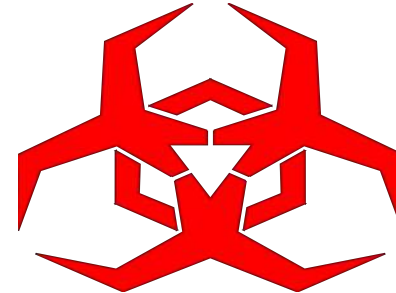
Default unlock price in BTC:

Default price is used when no rule matches.
0.6 BTC = 138 USD. Your affiliate reward is 0.42 BTC = 96 USD

Analysis of a Campaign: Upatre & Dyre

- Spam Email

- **From:** (random)
- **Subject:** Access All Areas Invoice
- **Attachment:** invoice.zip
- **VirusTotal Analysis Result:** 1/57



- User Execution

- **HTTP GET:** checkip.dyndns.org
- **HTTP GET:** 181.189.152.131/2602uk21/ADMIN-PC/0/61-SP1/0/KGBFDEBEJBFEL
- **HTTP GET:** alalihospital.com/ar/file/hone.pdf (data) **COMPROMISED SITE**
- **HTTP GET:** 181.189.152.131/2602uk21/ADMIN-PC/41/7/4/
- **TLS:** 194.28.191.217:443 TLS: Subject='C=CN, ST=ST...'
- **TLS:** 79.143.44.82:443 TLS: Subject='C=CN, ST=ST...'
- **HTTP GET:** 5.104.109.197/ml1from2.tar

- Final Payload

- **YvxRoVPD.exe**
- **VirusTotal Analysis Result:** 0/57

Analysis of a Campaign: Upatre & Dyre

- Spam Email
 - **From:** (random)
 - **Subject:** a1b2cDe3 - Your Quotation - matching /[0-9A-Za-z:]{8}/
 - **Attachment:** a1b2cDe3.zip
 - **VirusTotal Analysis Result:** **3/56**
- **User Execution**
 - **HTTP GET:** checkip.dyndns.org
 - **HTTP GET:** 141.105.141.87/3103uk11/DSHOUSE/0/61-SP1/0/KFBEBFBFDMBEHJ
 - **HTTP GET:** **dusanpacevac.rs/wp-content/.../2014/11/tus1.rtf (data) COMPROMISED SITE**
 - **HTTP GET:** 141.105.141.87/3103uk11/DSHOUSE/41/7/4/
 - **TLS:** 178.18.172.215:4443 TLS: Subject='C=CN, ST=ST...'
 - **HTTP GET:** **dynamicoffice.com.ar/.../tus1.rtf (data) COMPROMISED SITE**
- **Final Payload**
 - **YvxRoVPD.exe**
 - **VirusTotal Analysis Result:** **3/56**

Statistics of Upatre Campaigns

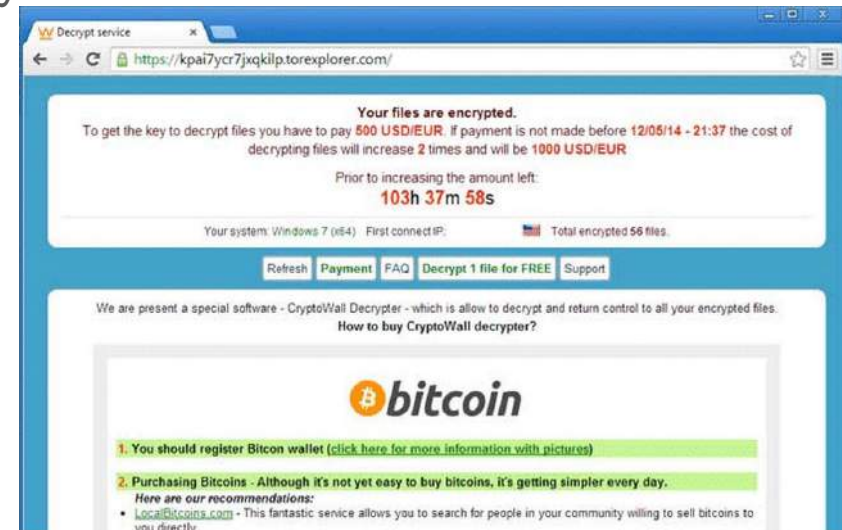
- **660,586 unique samples** since first delivery
 - First Seen: **2013-02-17 8:05:04am**
 - Last Seen: **2015-10-21 5:49:32am**
- **Primary Application Delivery Methods**
 - SMTP
 - POP3
 - Web Browsing
 - IMAP
- **618 unique samples** as of 9:00AM 2015/10/21
 - Unique samples; **traditional** Anti-Virus signatures

Analysis of a CryptoWall Campaign

- Drive-by **Fiesta Exploit Kit**
 - **Compromised Site:** <http://www.dbmotive.com/ora-12545-connect-failed-because-target-host-or-object-does-not-exist>
 - **HTTP Redirect:** <http://rgfgnrrv.hopto.org/tdstest/c1ba302e04a61816de2ec94839c5162f88/>
 - **HTTP Redirect:** http://rgfgnrrv.hopto.org/j_86zfsy/66d441210667479c...
(application/x-shockwave-flash)
 - **HTTP Redirect:** http://rgfgnrrv.hopto.org/j_86zfsy/43abe10cf7da0742...
(application/x-silverlight)
- **Payload CryptoWall v3.0**
 - **VirusTotal Analysis Result: 3/57**

Statistics of CryptoWall Campaigns

- **8,306 unique samples** since first delivery
 - First Seen: **2014-06-02 8:05:04am**
 - Last Seen: **2015-10-21 5:31:49am**
- **Primary Application Delivery Methods**
 - SMTP
 - Web Browsing
 - Flash Exploits
 - POP3
 - FTP
- **9 unique samples** as of 9:00AM 2015/10/21
 - No **traditional** Anti-Virus signatures



Closed-loop Threat Prevention

1

Reduce the attack surface

- Whitelist applications or block high-risk apps
- Block known viruses, exploits
- Block commonly exploited file types

2

Detect the unknown

- Analysis of all application traffic
- SSL decryption
- WildFire sandboxing of exploitive files

3

Create protections

- Detection and blocking of C&C via:
- Bad domains in DNS traffic
 - URLs (PAN-DB)
 - C&C signatures (anti-spyware)

