



INTELLIGENT CYBER THREAT RESPONSE

FireEye Intelligence Integration With Illuminate



Correlation

Aggregate and correlate all source intelligence. Gain visibility and extract unique indicators of compromise and characteristics of malicious cyber activity.



Operationalizing Intel

Comprehensive insight of cyber threats through awareness of the tools, techniques, and procedures employed by threat actors. Assess threats and exchange knowledge with partners.



Effective Action

We empower network defenders to more **effectively protect and operate** networked environments by simplifying the creation, execution and enforcement of countermeasures.

Reporting is sorted and prioritized

[illegible]

The screenshot displays the FireEye interface for a specific evidence item. The top navigation bar includes tabs for Activities, PDF Viewer, Automated Indicators, Associated Logs, History, and various system settings like Alerts, Dashboards, Malware, Cves, Assets, and Systems.

(U) Evidence: FireEye 17-00004607

File: `89e6dfe1c108d8f1`

Page: 12 of 17 | **Automate Scan:** Downloaded a second-stage previously undetected

- The second stage Trojan possesses anti-virus detection and evasion capabilities and will infiltrate the following data:
 - Operating System Information
 - Hostname
 - IP Address
 - CPU Information
 - RAM Usage
 - Size of PHYSICALDRIVE
 - List of anti-virus applications that are currently running

MD5: `00ef14ad20761ee14436789e` **SHA1 File Downloader:** `00ef14ad20761ee14436789e` **Stage-Two Trojan Contact IP:** `92.63.103.70`

Source: 2018 Trojan - No Anti-Virus

Query Results | Query Virus Total | Inherit Evidence TLP | Highlight All

Type:	Domain:
Indicators: Undetected	malicious.rightnet.com
Class:	Class: U
Benchmark:	Class: U
Risk:	Class: U
Domain Registration:	Domain Name: rightnet.com Registry Domain ID: 2177844293_DOMAIN_COM-VRSN
IP Resolution:	92.63.103.70 Class: U
Registration:	<p>No Abuse contact for '92.63.96.0 - 92.63.103.255' is listed at abusecontact.org</p> <p>ip: 92.63.96.0 - 92.63.103.255 network: rightnet.net asn: OIG-FYDRL-APE org: TheFBI-US-stake (TheFBI-WAC MA) country: RU city: PASTA-RU tech-c: PASTA-RU admin-c: ASGSDIO AKA mnt-by: THEFBI-ST-MNT</p>
Description:	Class: U
Class:	Class: U

FireEye **THREAT INTELLIGENCE**

External	Internal
603da43cd2676132a55925567fa02ba6d	csl@csail.mit.edu
23b6d81cbe67192696237db6dc5b89	secmon.payalysite.com
7f535b085374ea373e1d916ae47ac8	pauline@rightnet.com

Note: Table 7. Related Infrastructure

Notably, domain registration emails associated with the above infrastructure are consistent with previous Ransom Team infrastructure that uses "theftcs.co.jp" for registration purposes (LE-000008020). Given their linkage to ongoing Ransom Team operations, future domains registered upon these emails should be considered relevant in nature.

Related Infrastructure:

- `csail@csail.mit.edu` | `csail@csail.mit.edu`
- `secmon.payalysite.com` | `secmon@payalysite.com`



(U) Evidence: FireEye 17-00004607

Attributes PDF Viewer Associated Indicators Associated Rules History

Indicator Extractions **Filter**

ID	Type	Value	Evidence ID	Valid Class	Source	ET Reported	Last Reported	MALWARED	File Name	Digital Signature ID
536851	HTTP Request	/pentos.io	8	U	Raining Tiger	11/20/2016	01/04/2018	ENFAL	Undetermined	White
28857	Domain	vuln.com	7	U	Pearson, Raining Tiger, Unknown	10/01/2015	12/10/2017	ENFAL	Undetermined	Undetermined
165795	Domain	185.92.120.80.vuln.com	1	U	Raining Tiger	05/10/2017	05/10/2017	ENFAL	Undetermined	Undetermined
165792	Domain	158.61.197.100.vuln.com	1	U	Raining Tiger	05/10/2017	05/10/2017	ENFAL	Undetermined	Undetermined
165789	Domain	158.61.117.139.vuln.com	1	U	Raining Tiger	05/10/2017	05/10/2017	ENFAL	Undetermined	Undetermined
165787	Domain	vuln.dreaded.com	1	U	Raining Tiger	05/10/2017	05/10/2017	ENFAL	Undetermined	Undetermined
165786	Domain	pulled-right.net	1	U	Raining Tiger	05/10/2017	05/10/2017	ENFAL	Undetermined	Undetermined
165780	IPv4	158.61.117.205	1	U	Raining Tiger	05/10/2017	05/10/2017	ENFAL	Undetermined	Undetermined
165779	Email	yehavi@2drevolve.co.jp	1	U	Raining Tiger	05/10/2017	05/10/2017	ENFAL	Undetermined	Undetermined
165733	Email	jenshi@revolve.co.jp	1	U	Raining Tiger	05/10/2017	05/10/2017	ENFAL	Undetermined	Undetermined

Illuminate introduces automation to reduce time-consuming tasks and establishes a shared knowledge base that captures analysis and actions throughout the cyber defense process.