

# COMBATING CYBER THREATS IN HIGHER EDUCATION

Aaron Baillio, Sec+, CEH, CISSP  
Managing Director, Security Operations and Architecture  
University of Oklahoma

# Agenda

- Setting the stage
- The University of Oklahoma
- Is it Education or a Business?
- How are other Universities stacking up?
- Our Security Methodology
- Threat Intel and How it Applies
- Room for Improvement

# Setting the stage

- “Can Campus Networks Ever be Secure?”
  - Josephine Wolff, The Atlantic.com, Oct 2015
- Enterprise Networks
  - Highly secure networks that regulate and restrict new devices, users and networks.
  - Good for guarding secrets: government, corporate and intellectual property.

# Setting the Stage

- Educational Networks
  - University networks aren't designed to protect secrets.
  - We draw “intellectual sustenance” from the turnover, the arrival of new people and the exchange of thoughts and ideas.
  - There is a balance between allowing the free exchange of information and protecting users and the sensitive data of the University.

# The University of Oklahoma

- OU Enrollment in 2014
  - 1,998 International Students
    - Sub-Saharan Africa – 170
    - Asia – 1,066
    - Europe – 294
    - Latin America – 170
    - Middle East & N. Africa – 242
    - North America – 37
    - Australia – 15
    - Stateless – 4

# The University of Oklahoma

- International Students from (a sample):
  - China
  - Japan
  - Afghanistan
  - India
  - Cambodia
  - Latvia
  - Serbia
  - Libya
  - Syria
  - Iran
  - Botswana
  - Philippines
  - Turkey
  - Ukraine
  - Zambia

# The University of Oklahoma

- Study Abroad
  - 82 Countries
  - 240 Cities
  - 6 Continents
- Faculty are traveling across the world.
- We have visiting faculty who:
  - Need accounts
  - Need access
  - Need VPNs

# The University of Oklahoma

- International Students account for 8.3% of total enrollment for the Norman campus.
- Total enrollment 2014 – 24,044
  - One of America's Best 100 Buys determined by Institutional Research & Evaluation.
  - 227 acre research campus with specialties in:
    - Radar technology
    - Meteorology
    - Genetics
    - Energy
    - Life Sciences



# The University of Oklahoma

- OU's research campus was named #1 research campus in the nation in 2013.
- OU ranks #1 in the nation in enrollment of National Merit Scholars.
- One of America's Top 25 Most Beautiful Campuses.
- Fall to fall retention this year at 90% - highest ever in school history.

# The University of Oklahoma

- 24,044 students & 4709 faculty/staff
  - All bringing new devices
  - Each student has on average 5 devices
  - New, unique DHCP leases for Aug 2016 projected to hit over 100,000
  - Roughly 22,000 devices on the wireless network when school is in session

# The University of Oklahoma

- Devices:
  - No baseline OS, patch level or SP
  - Must support most internet connected devices
  - Wired and wireless
- People:
  - Flux of people from all over the world
  - Students ages 17-???
  - Bored, untrained, curious
- Equals:
  - Lots of interesting traffic!!!
  - Malware and infections

# Business or Academia?

As a security professional, what am I protecting in this environment?

- Personally Identifiable Information (PII)
  - Human Resources, Administration, Finance
  - Faculty Advisement
- Family Educational Rights & Privacy Act (FERPA)
  - Can't disclose educational information without consent
  - PII/Directory information coupled with a grade
  - Faculty notes on student performance, etc.

# Business or Academia?

- Payment Card Industry (PCI)
  - Concessions at Athletics events / Pro Shop
  - OU Book & Clothing stores
  - Vendors
  - Room & Board
  - Payroll / Direct Deposit
- Health Insurance Portability and Accountability Act (HIPAA)
  - OU Health Sciences Center
  - Health clinic on campus
  - Athletics and support departments



# Business or Academia?

- Intellectual Property
  - Research data
  - Subscriptions to 3<sup>rd</sup> party data/record repositories
- Other Sensitive Data
  - Faculty tenure advancement
  - Recruitment & retention methods
  - Game play video, play books, tactics

# Business or Academia?

- Federal Grants
  - Federal Information Security Management Act (FISMA)
  - Export controlled data – International Traffic in Arms (ITAR)
  - National Industrial Security Program Operating Manual (NISPOM)

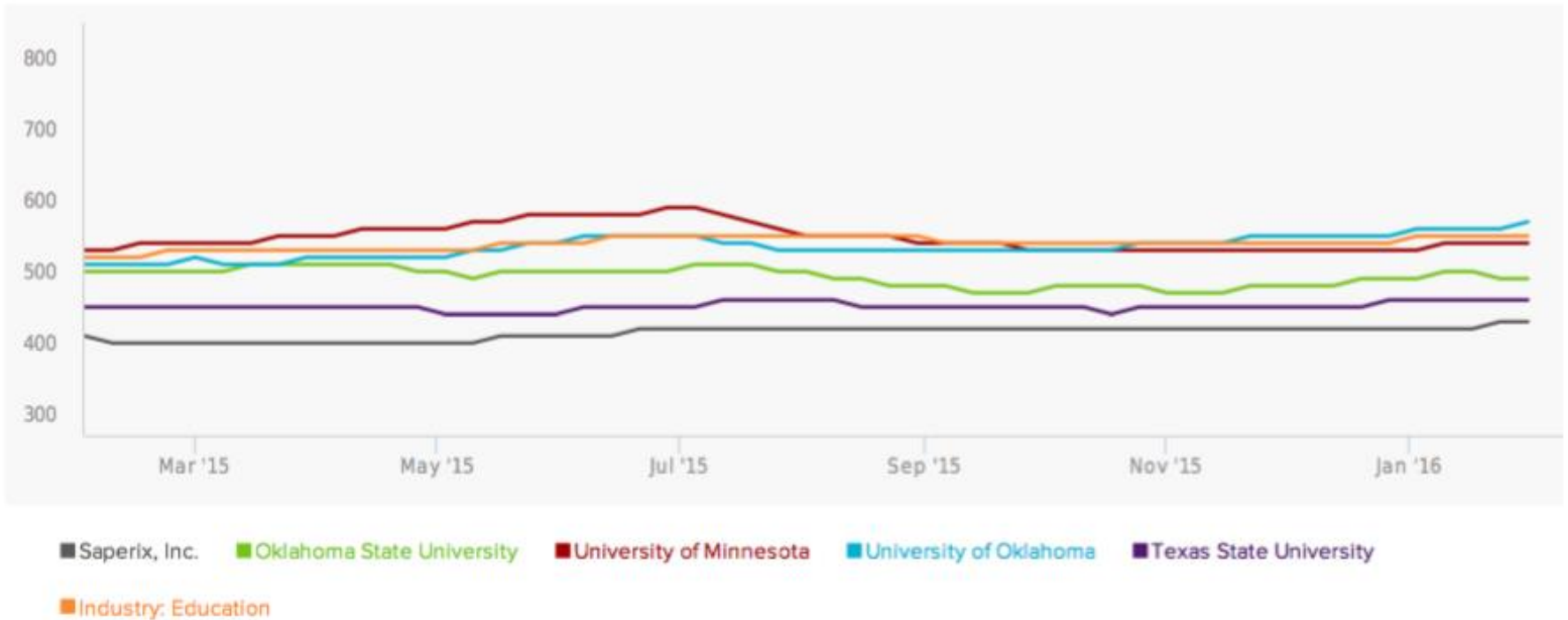
# Business or Academia?

- PII, PCI, HIPAA, Intellectual Property, FISMA
- Looks just like a corporation right?
- Target rich environment
  - All of the above regulated data types
  - Student personal information
    - Excellent or new credit histories
    - Easy pivot points to institutional data
- How do educational institutions traditionally fare in security performance?



# How is Academia Stacking Up?

## HISTORICAL COMPARISON



# How is Academia Stacking Up?

- 2013 – New York Times reports a breach. Mandiant found that the attacks were routed through Universities.
- Jun 2015 – Harvard discovered a breach in the Faculty of Arts and Sciences and Central Administration.
- Jul 2015 – University of Connecticut responds to a criminal cyber intrusion originating in China.

# How is Academia Stacking Up?

- Dec 2015 – U.C. Berkley reports 80,000 records exposed during a cyber attack on their financial system.
- Feb 2015 – University of Oklahoma's College of Business has several databases compromised after a racial incident with the SAE fraternity.
- Academia is now ranked 3<sup>rd</sup> in the top 10 of industries breached.

# How is Academia Stacking Up?

- So....
- Academia is not immune or flying under the radar.
- "University networks often have multiple levels of connectivity and accessibility to enable research, collaboration and an 'open culture' among faculty and students." - Dept. Homeland Security

# How is Academia Stacking Up?

- How do we balance allowing access and academic freedom with protecting the corporate aspect of the University?
- What techniques can be leveraged for a security organization fighting against a culture used to open protocols and access?













# Our Security Methodology




- Our Security Trinity:
  - Threat Intelligence
  - Adaptive Technologies
  - Resilient Processes
- How are we leveraging threat intelligence?
  - Manual processes
  - Integrations
  - Sharing

# Threat Intel – Manual Processes

- HUMINT
  - CoIT Oklahoma
  - REN-ISAC
  - EDUCAUSE
  - Infraguard
  - Other Federal and/or Media publications
- Manual Processes
  - Manual IoC lookups
    - Threat Stream
    - Virus Total
    - Other

# Threat Intel – Manual Processes

 Trojan infection	XCodeGhost	<b>HIGH</b>	N/A	10.204.231.8:64727	mc2:domain	
 Trojan infection	VOPackage	<b>HIGH</b>	N/A	Host-129-15-64-216:52110	 54.221.205.146:http	
 Malicious website	Phishing activity	<b>HIGH</b>	N/A	Host-129-15-88-45:38267	 54.235.75.253:http	
 OTX Indicators of Compromise	Cross-Platform Adware; OSX/Pirrit	<b>HIGH</b>		 204.194.238.11:51163	 129.15.0.146:domain	
 Adware infection	InstallCore	<b>HIGH</b>	N/A	Host-129-15-66-167:50774	 184.72.252.168:http	

9 hours   Trojan infection XCodeGhost **HIGH** N/A 10.204.231.8:64727 mc2:domain 



**SYSTEM COMPROMISE: TROJAN INFECTION**  
ATTACK PATTERN: EXTERNAL TO INTERNAL ONE-TO-ONE

OPEN & CLOSED ALARMS



TOTAL EVENTS

1

2016-08-30 14:39:09

DURATION

2

HOURS

ELAPSED TIME

9

HOURS

[VIEW DETAILS](#)

[CLOSE](#)

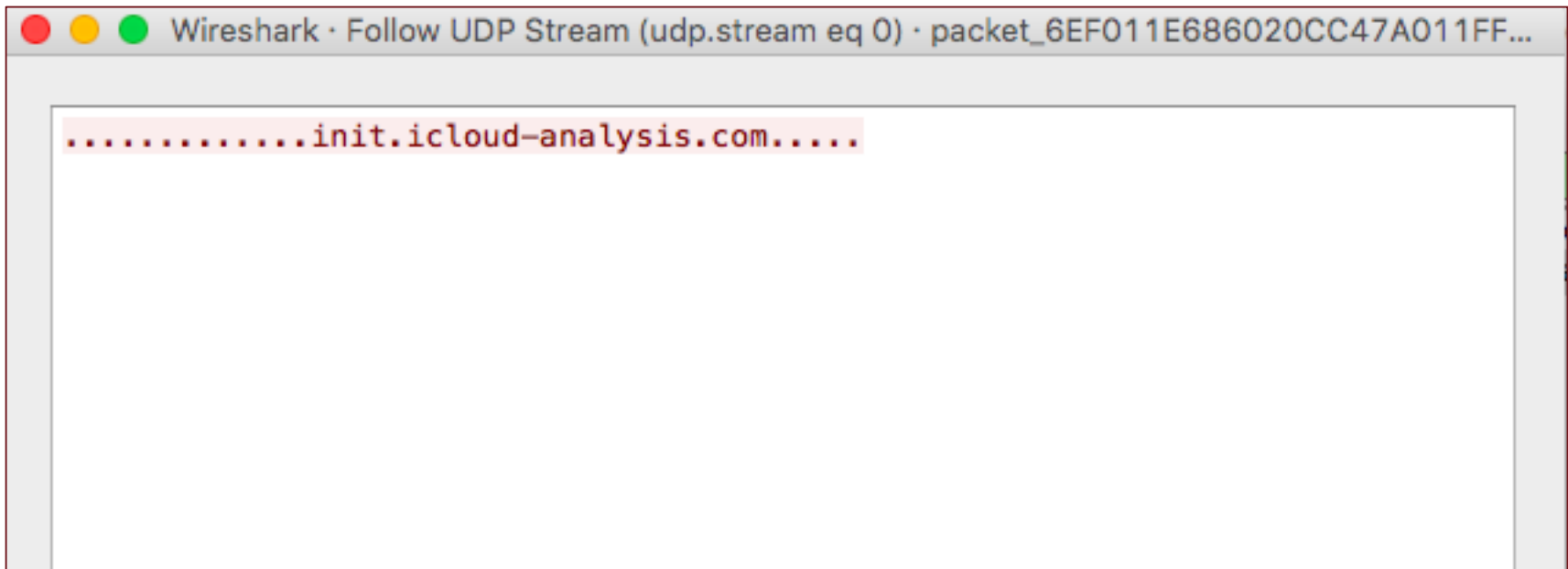
[DELETE](#)

[APPLY LABEL](#)





# Threat Intel – Manual Processes



# Threat Intel – Manual Processes

## Search Results for init.icloud-analysis.com

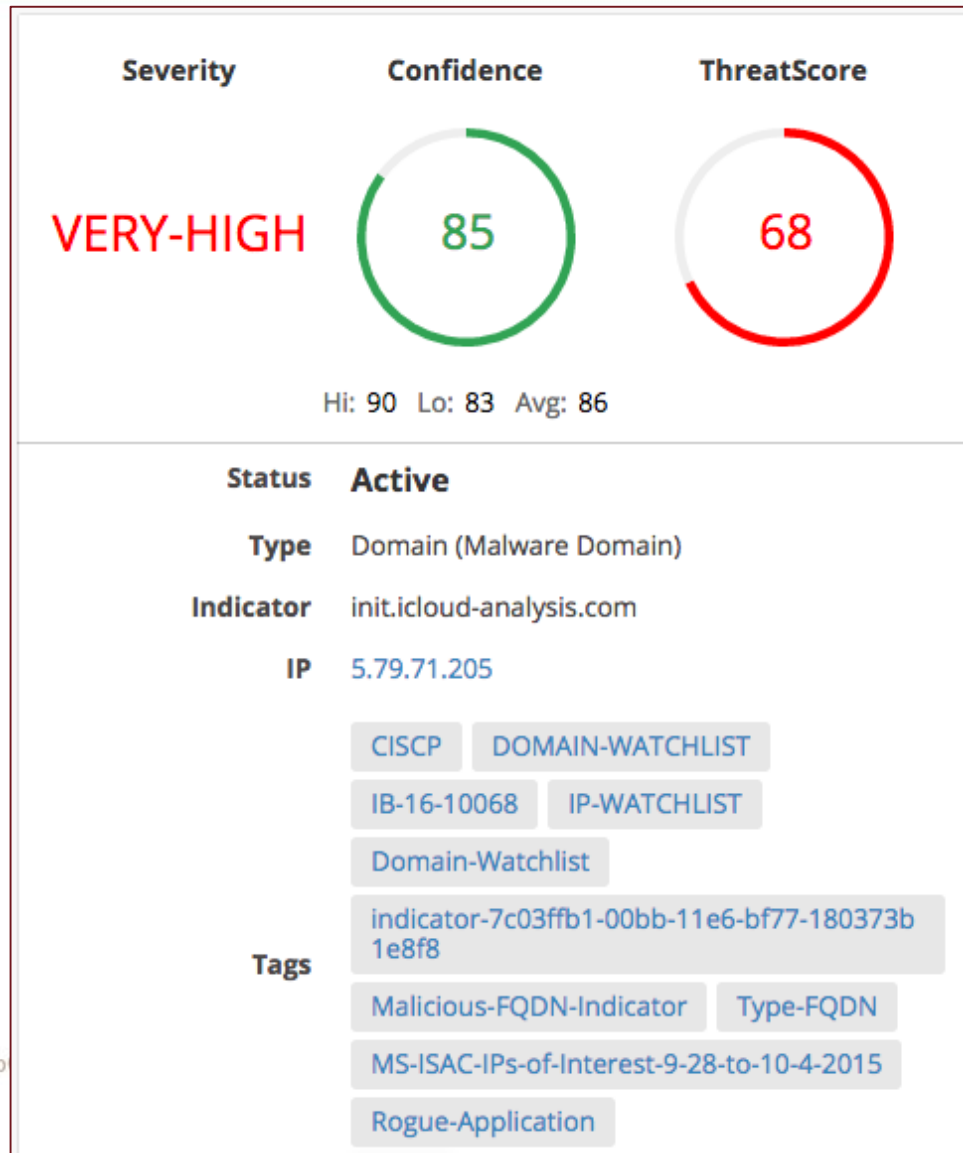
### Indicators

Status **ACTIVE** ✖

Date First	iType	Indicator	Country	Source	Classification	Tags
2016-06-08 22:19:05	Malware Domain	<a href="http://init.icloud-analysis.com">init.icloud-analysis.com</a>	NL 	CISCP STIX/TAXII	CISCP	Domain-Watchlist indicator-7c03ffb1-00bb-11e6-bf77-180373b1e8f8 Malicious-FQDN-Indicator Type-FQDN

[See more in Search](#)

# Threat Intel – Manual Processes



# Threat Intel – Integrated Solutions

- Threat Intel Integrated Solutions
  - AlienVault OTX
  - REN-ISAC
  - Anomali ThreatStream
  - Cisco ThreatGrid
  - Palo Alto Wildfire
  - IBM X-Force
  - FireEye NX

# Threat Intel - Integrations

- Platform Centric Integrations
  - AlienVault OTX



2016-08-28 17:48:25 open OTX Indicators of Compromise Cross-Platform Adware; OSX/Pirrit **HIGH** Host-129-15-64-232:27452 130.117.78.253:http

ENVIRONMENTAL AWARENESS: OTX INDICATORS OF COMPROMISE  
ATTACK PATTERN: INTERNAL TO EXTERNAL ONE-TO-ONE

OPEN & CLOSED ALARMS	TOTAL EVENTS	DURATION	ELAPSED TIME
-----	2	20	9
	2016-08-28 17:48:25	SECS	DAYS

[VIEW DETAILS](#)  
[CLOSE](#)  
[DELETE](#)  
[APPLY LABEL](#)

# Threat Intel - Integrations

### OTX DETAILS

OTX Pulse: Cross-Platform Adware; OSX/Pirrit

Cross-Platform Adware; OSX/Pirrit

MacOSX Malware OSX/Pirrit


**OTX Indicators of Compromise:**

SHOW 5 INDICATORS

TYPE	INDICATOR
domain	aa625d84f1587749c1ab011d6f269f7d64.com

SHOWING 1 TO 1 OF 1 INDICATORS FIRST PREVIOUS 1 NEXT LAST

# Threat Intel - Integrations



## Cross-Platform Adware; OSX/Pirrit

CREATED 151 days ago by AlienVault | Status: Public | TLP Classification: Green

MacOSX Malware OSX/Pirrit

REFERENCES: h


TAGS: os x, mac, adware, mac os x, OSX/Pirrit, Pirrit, cybereason

GROUPS: No groups. Add to Group

18K SUBSCRIBE 0 COMMENTS 0 RELATED PULSES

SUGGEST EDIT CLONE DOWNLOAD EMBED

### Summary



TYPES OF INDICATORS

### Indicators of Compromise

Show 10 entries Search:

TYPE	INDICATOR
domain	93a555685cc7443a8e1034efa1f18924.com
domain	aa625d84f1587749c1ab011d6f269f7d64.com
domain	2ff328dcee054f2f9a9a5d7e966e3ec0.com
domain	trkitok.com
domain	aae219721390264a73aa60a5e6ab6ccc4e.com
FileHash-MD5	85846678ad4dbff608f2e51bb0589a16
FileHash-MD5	70772fccaec011be535d1f41212f755f

SHOWING 1 TO 7 OF 7 ENTRIES < PREVIOUS 1 NEXT > ADD INDICATORS

# Threat Intel - Integrations

- Platform Centric Integrations
  - Cisco ThreatGrid
    - OpenDNS
    - CloudLock (future integration)

SEARCH

PATTERN SEARCH

init.icloud-analysis.com

INVESTIGATE

## ASSOCIATED SAMPLES

POWERED BY CISCO AMP THREAT GRID

Threat Score	SHA256 Signature	AV Result
56	72e6e8b14fced82c15f55e085a781414b4ec14d502d329beb059826454670f6b	

1-1 of 1





# Threat Intel - Integrations

[SEARCH](#) [PATTERN SEARCH](#)

[INVESTIGATE](#)

**THREAT SAMPLE (SHA256)**  
**72e6e8b14fced82c15f55e085a781414b4ec14d502d329beb059826454670f6b**

SHA1 5defd092efbf1f403cf3b01ea84186e061a2b71a  
MD5 4a33f9e1e94ed4c312004a4fb14184f6

Threat Score: **56**

Magic Type: MS Windows 95 Internet shortcut text (URL=< >), ASCII text  
Size: 55 bytes  
First Seen: May 5, 2016 13:23:51 UTC  
Full Sample Data from Threat Grid

**BEHAVIORAL INDICATORS**

Indicator	Severity ⓘ	Confidence ⓘ
Process Modified File in a User Directory	70	80
File Downloaded to Disk	30	90
DNS Response Contains Low Time to Live (TTL) Value	35	20
Outbound HTTP GET Request From URL Submission	25	25

**NETWORK CONNECTIONS**

Destination	URLs	Security Categories
init.icloud-analysis.com (178.162.217.107 & 7 more)	2 ▾	Malware
ie9cvlist.ie.microsoft.com (72.21.81.200)	1 ▾	
iecvlist.microsoft.com (72.21.81.200)		

1-3 of 3 < >

# Threat Intel - Integrations

## – Palo Alto Wildfire

Received Time	Source	File / URL	Verdict
2016-09-04 20:55:08	009908000353	DHL_Receipt.exe	Malware
2016-09-04 10:21:32	009908000353	92.240.238.39/1/source/crypserv.exe	Malware
2016-09-04 09:53:07	009908000353	dl.samplayeedmed.com/download/dwn/firas/en/setup_mpck_en.exe	Malware
2016-09-04 09:48:05	009908000353	bscdn.pw/downloads/weboptimum/produrl/1_10fb/cl5/WebOptimumSetu	Malware
2016-09-04 03:20:03	009908000353	skipsoft.net/download/toolkit/unifiedandroidtoolkit/devicefiles	Malware
2016-09-04 03:19:43	009908000353	skipsoft.net/download/toolkit/unifiedandroidtoolkit/devicefiles	Malware
2016-09-01 07:06:43	009908000353	Scan Document.exe	Malware

# Threat Intel - Integrations

## WILDFIRE ANALYSIS REPORT

[Download as PDF](#)

### FILE INFORMATION

File Type	PE
File Signer	
SHA-256	051655cbc53559a5ac19052e8fb08f9154bf868c5b12e30b851fde6c04b7d35f
SHA-1	8f76e5f68e0e39e8076be3d344a1fba83eb37c3a
MD5	bf01496c0eba752b9a5be7410635cf15
File Size	147456 bytes
First Seen Timestamp	2016-09-03 17:55:30 CDT
Sample File	<a href="#">Download File</a>
Verdict	<b>Malware</b>

### SESSION INFORMATION

File Source	92.240.238.39:80
File Destination	10.193.20.225:60071
User-ID	unknown
Timestamp	2016-09-04 10:21:32 CDT
Serial Number	009908000353
Firewall Hostname/IP	PA-7050-1PP
Virtual System	5
Application	web-browsing
URL	92.240.238.39/1/source/crypserv.exe
File Name	crypserv.exe

### COVERAGE STATUS

The table below lists all coverage related to this malware sample. For endpoint antivirus coverage information for this sample, visit [VirusTotal](#)

Previous 1 Next

Coverage Type	Signature ID	Detail	Date Released	Latest Content Version
virus	2390659	Virus/Win32.WGeneric.jquyq	2016-09-05T20:10:27	1991



INFORMATION  
TECHNOLOGY




# Threat Intel - Integrations

- IBM X-Force
  - Resilient Incident Response Platform

Artifacts

Show Types **All** ▾ **Add Artifact**

**Table** **Graph**

Type	Value	Created	Actions
 <b>Malware MD5 Hash</b>	e9ffdb716af3d355b25096a8ed4de8ef	08/23/2016	Delete 
 <b>Malware MD5 Hash</b>	8604e0f263922501f749cfca447b041a	08/23/2016	Delete 

# Threat Intel - Integrations

8604e0f263922501f749cfca447b041a Artifact ✕

---

**Details** Edit

---

Created 08/23/2016 15:42  
Created by [Aaron Baillio](#)  
Value 8604e0f263922501f749cfca447b041a  
Type **Malware MD5 Hash**  
Description -

---

**Hits (3)**

---

**IBM X-Force Exchange**

Anti-virus engines detection	62%
Malware family	heuristic; trojan
Permalink	<a href="https://exchange.xforce.ibmcloud.com/malware/8604E0F263922501F749CFCA447B041A">https://exchange.xforce.ibmcloud.com/malware/8604E0F263922501F749CFCA447B041A</a>

---

**Virus Total**

Detection Ratio	34 / 56 antivirus engines
Report Url	<a href="#">VirusTotal Scan Report</a>

---

**IBM X-Force Exchange**

Anti-virus engines detection	61%
Malware family	heuristic; trojan
Permalink	<a href="https://exchange.xforce.ibmcloud.com/malware/8604E0F263922501F749CFCA447B041A">https://exchange.xforce.ibmcloud.com/malware/8604E0F263922501F749CFCA447B041A</a>

# Threat Intel - Integrations

## – FireEye NX

File Type:	zip
Original analyzed at:	09/11/16 07:47:34
Yara rule:	■ FE_Suspicious_Zip_d5dc
AV Suite:	■ Trojan.Downloader.VBS

### Advanced Threat Intel [More Info](#)

Last Updated: 04/05/2016 08:03

#### Event Summary

Name	Downloader.DTI.Heuristic
MD5 SUM/URL	8604e0f263922501f749cfca447b041a
Threat Level	Medium
Threat Type	Downloader
Attribution	This threat may be used by cybercrime, APT, or may be associated with a potentially unwanted program. This detection may be updated as more information is available and correlated by FireEye Dynamic Threat Intelligence..
Risk Summary	This threat is detected through static or behavioral heuristic analysis. It is likely that this threat exhibits known traits of suspicious behaviors and features, or shares code similarities with malware. This binary has been observed in attacks against the following industries: Education, Financial Services, and Manufacturing. This binary has been observed in attacks against the following countries: United States and Germany.

# Threat Intel - Integrations

- Platform Agnostic Integrations
  - Bro IDS
    - Threat Stream
    - AlienVault OTX
  - Palo Alto
    - Threat Stream
    - Other
  - Resilient
    - Custom Threat Plugins

# Room for Improvement?

- Each threat intel source helps provide information that allows the security team to prioritize.
- While there are similarities across platforms, usefulness, detail and efficacy vary across platforms.
- It is still difficult for a small staff to prioritize across platforms.



# Feature Request

- More synchronization between threat intel sources and/or between platforms.
- There is a movement in IT Security to move beyond technology silos and share information.
  - E.g. Malware makes it past firewall/IPS, past the network detection/sandbox tool but is caught by the endpoint agent. The endpoint then sends the intel back up the chain so it's blocked in the future.

# Conclusion

- Academic networks face many of the same attacks as corporate networks.
- Threat intelligence is a key tool in both allowing and supporting academic freedom while also providing the insight to address real security threats.
- Convergence of threat intel across security platforms will allow for the adaptive defenses required to adequately prevent and react to actual cyber attacks.

# Conclusion