HITRUST
Health Information Trust Alliance

Monthly Cyber Threat Briefing

June 2016

Presenters

- **US-CERT:** Majed Oweis, CISCP Analyst
- **Armor:** Charity Willhoite, Intelligence Analyst
- **Trend Micro:** Jon Clay, Global Threat Communications
- **HITRUST:** Dennis Palmer, Senior Assurance Associate

NCCIC/US-CERT REPORT

TLP: GREEN – JAR-16-20114 – Widespread Advanced Persistent Threat Activity Targeting the Private Sector and the Federal Government

TLP: GREEN – JAR-16-20126– Recommended Mitigations for Institutions with Connections to Payment Messaging Systems

TLP: GREEN – JAR-16-20114 – Widespread Advanced Persistent Threat Activity Targeting the Private Sector and the Federal Government

- Collaborative effort between DHS/NCCIC/US-CERT and the FBI.
- Based on information obtained by DHS and the FBI regarding APT groups' cyber espionage against U.S. commercial and government networks.
- Tools used by the adversaries include HiKit, WINNTI, Derusbi, Plug-X, and HomeUnix.
- Noted sign of intrusion to look for is self-signed SSL/TLS traffic.
- The JAR includes recommended mitigations and two appendices:
  - Appendix A - indicators of compromise (IOCs).
  - Appendix B – A Snort signatures and YARA rules.

TLP: GREEN – JAR-16-20126– Recommended Mitigations for Institutions with Connections to Payment Messaging Systems

- Collaborative effort between DHS/NCCIC/US-CERT and the FBI.
- Malicious cyber group activity led to the compromise of the networks of foreign banks.
- The actors exploited vulnerabilities of internal network elements connected to their local interface to the international payment messaging system network. The result was unauthorized money transfers taking place over the international payment messaging system
- The malware used appears to have been customized for each victim environment.
- The malware used appears to have been able to remove traces of messages that were sent, and was able to delete itself upon task completion.
- The report includes a recommended mitigation strategy, and an appendix that includes IOCs, YARA rules, and a snort signature.

The reports are located at:

- **JAR-16-20114:**
  - https://portal.us-cert.gov/documents/70338/108826/JAR-16-20114.pdf/f81266d0-dc49-4859-9252-70ef51d8c90f
- **JAR-16-20126:**
  - https://portal.us-cert.gov/documents/70338/108826/JAR-16-20126.pdf/69da4c06-776f-4d2c-be56-f79f2d25b11d

Questions? Comments?

Contact US-CERT at:

- Email: soc@us-cert.gov
- Phone: 1-888-282-0870
- Website: www.us-cert.gov

Contact CISCP at: CISCP@us-cert.gov

Top Threat Trends and Defenses

ARMOR

Trending Vulnerabilities

NAME	RISK SCORE	FIRST SEEN	RELATED TECH
CVE-2016-4328	10/10 Critical	6/9/16	MEDHOST PIMS/VPIMS before 2015R1
CVE-2016-2343	9.8/10 Critical	2/19/16	Patterson Dental Eaglesoft 17
CVE-2016-2208	9.4/10 Critical	5/19/16	Symantec AV Engine 20151.1.1.4
CVE-2010-3333/ MS10-087	9.3/10 Critical	11/9/10	MS Office 2003-2011, PC, Mac
CVE-2016-0800	5.9/10 Medium	3/1/16	SSLv2 protocol, OpenSSL before 1.0.1s and 1.0.2g

Action Items:

- MEDHOST: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2343
- Patterson Dental Eaglesoft: http://www.kb.cert.org/vuls/id/344432
- Symantec: https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&suid=20160516_00
- MS Office: https://technet.microsoft.com/library/security/ms10-087
- OpenSSL update: https://www.openssl.org/blog/blog/2016/03/01/an-openssl-users-guide-to-drown/

Top Emerging Malware

NAME	Category	RELATED TECH, Industries, Indicators
Qarallax	RAT	Skype, F Secure Oyj, Quaverse, US government, US DOS, Immigration, Travel
Zycode	Phishing Kit	Apple ID, iTunes, iCloud, Phishing, JavaScript, HTML, Suspicious domain registration
Cerber	Ransomware	Adobe Flash, MS Windows Vista, DDoS, polymorphic malware

Action Items:

- Preserve your data: Frequent data backups!
- Security Awareness: Don't click on attachments and links you don't recognize!

Top US Healthcare Targets: May–June 2016

Organization	Individuals Impacted	Type of Breach
Stamford Podiatry Group	40,491	Hacking/IT Incident
Integrated Health Solutions PC	19,776	Hacking/IT Incident
San Juan County New Mexico	12,500	Hacking/IT Incident
Complete Chiropractic & Bodywork Therapies	4,082	Hacking/IT Incident
Allen Dell, P.A.	2,500	Hacking/IT Incident
Melanie Witte (counsel for Berkeley Endocrine Clinic)	1,370	Unauthorized Disclosure/Access (Email)
Emergency Room Associates doing business as Emergency Medicine Associates	1,067	Theft (Paper/Films)
Washington DC VA Medical Center	1,062	Theft (Paper/Films)
Aflac	930	Unauthorized Access/Disclosure
Keystone Rural Health Consortia, Inc.	800	Theft (Electronic Records)

Action Items: Implement least-privilege policies, set complex passwords, conduct security awareness training emphasizing the need to secure equipment and files

Emerging Threats: IP Block List

IP Address	Risk Score	Malware	Behavior Observed
213.186.33.19	90%	Malware C&C IP	Malware, phishing, spamming
216.185.114.219	90%	DarkComet Trojan	RAT C&C IP
195.88.243.196	90%	DarkComet Trojan	RAT C&C IP
74.208.153.26	90%	DarkComet Trojan	RAT C&C IP
91.224.160.10	87%	N/A	Brute Force SSH
61.191.61.142	77%	N/A	Slow SSH Attack, Brute Force
113.57.232.34	73%	N/A	Brute Force SSH
106.184.2.29	71%	N/A	Brute Force Telnet
197.239.33.22	71%	N/A	Brute Force Intrusion
222.186.34.74	70%	N/A	Brute Force Intrusion
98.124.199.1	65%	Malware C&C IP	Suppobox, APT IP

FastPOS: Quick and Easy Credit Card Theft

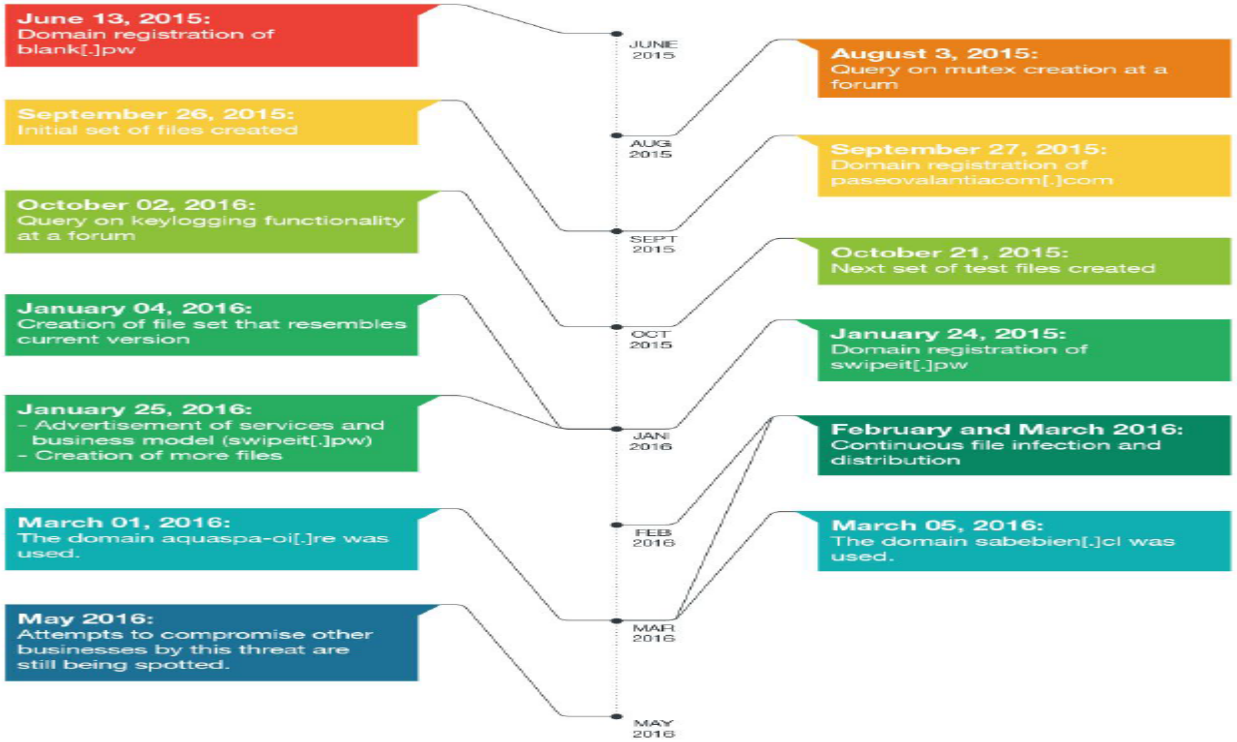
TREND MICRO

Infection Vectors

FastPOS (detected as TSPY_FASTPOS.SMZTDA)

- Links to a compromised medical site talking about laser surgical techniques
- A real-time file sharing service
- Direct file transfer via VNC

Timeline



Victim Locations

Taiwan	Japan	Hong Kong	Brazil	France	United States
					
					

Information Theft

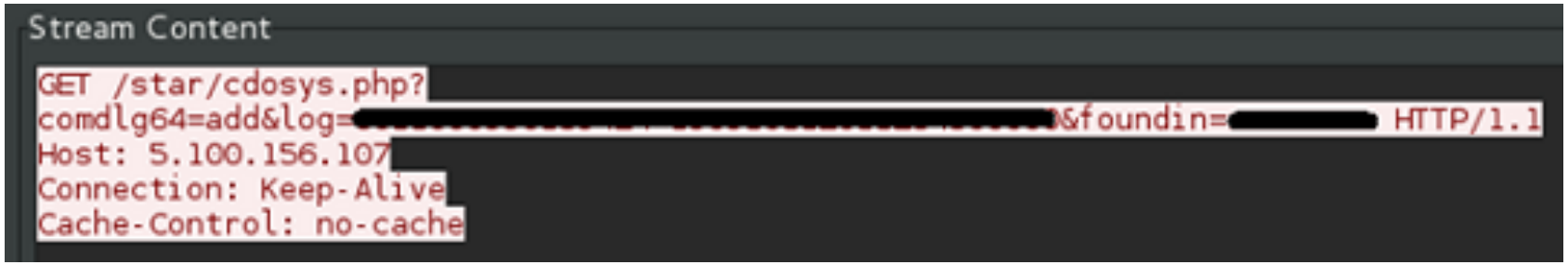
- Focuses on sending stolen data immediately to actor
- Includes both RAMscraping and Keylogging
  - Keylogger data stored in memory
  - Stolen information can include user credentials, personally identifiable information (PII) of customers and staff, all the way to payment information. (To help attackers figure out which is which, the title of the window where these keystrokes were stolen from is also logged and included with the data.)

Ramscraper

- The RAM scraper is designed to steal only credit card information.
- A series of checks are meant to ensure that the RAM scraper is able to steal valid card numbers.
- Uncommon feature
  - Verification of the card's service code.
  - A card with either the 101 or 201 service codes can be used normally around the world.
  - The only difference is that the 201 service code specifies that the on-board chip of newer EMV cards must be used, where feasible.
  - Cards that require PINs for transactions are also excluded.

Data Exfiltration

- Stolen information is immediately uploaded to a C&C server
- The location is hardcoded inside the malware



Exfiltration Commands

key&log=TWND%sKWND%s	Used to send the logged keystrokes. First string is the window title; second string is the key log
add&log=%s&foundin=%s	Used by the RAM Scraper thread during data exfiltration. First string is the card dump; second string is the process name.

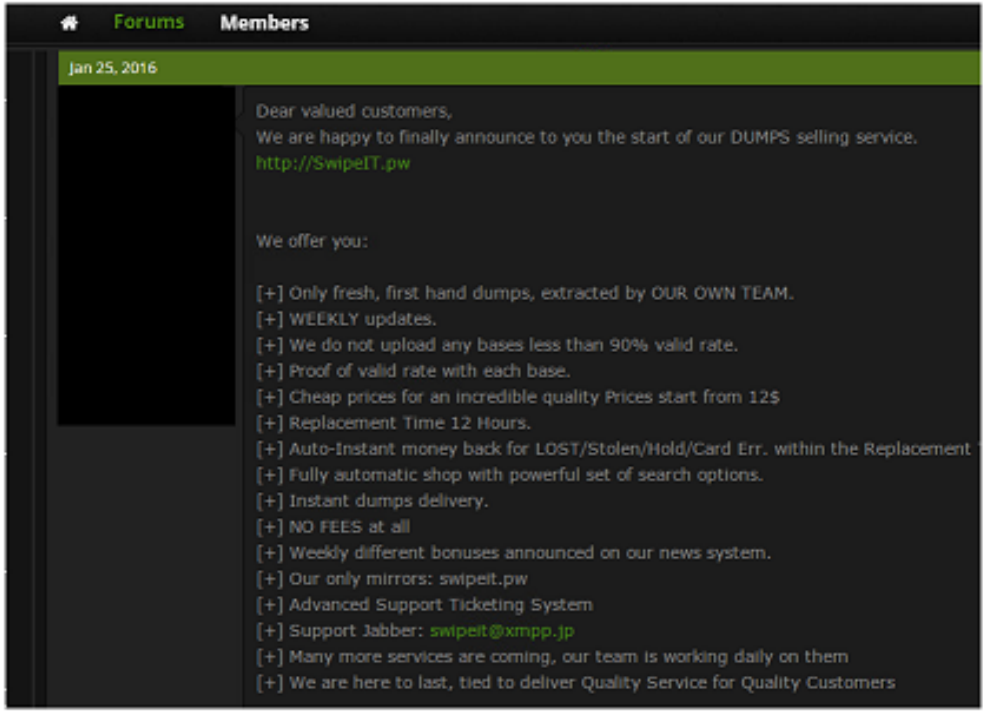
Table 1. Exfiltration commands

Exfiltration Commands

new&username=%s&computername=%s&os=%s&architecture=%s	Registers new infected system with user name, computer name, OS and architecture
statuslog&log=scanning-%s	Indicates processes being scanned for credit card data
update&username=%s	Sent when a software update is requested
statuslog&log=CheckedForUpdate	Sent after request for software update
statuslog=&log=GetLastError%d	Reports encountered error with an error code

Table 2. Other commands

Threat Actor



- Ad is for a site where other users can buy stolen card information.
- The site's IP address used by FastPOS itself as a C&C server too
- FastPOS actor(s) are selling stolen credentials via the same server they use to receive these credentials.

Insights

- FastPOS's design sets it apart from other POS malware families.
- Appears to be designed to operate in situations where a large, enterprise-scale network may *not* be present:
- Designed for environments with a much smaller footprint. This could be cases where the primary network gateway is a simple DSL modem with ports forwarded to the POS system.
- Detailed Technical details including IoC:
  - http://documents.trendmicro.com/assets/fastPOS-quick-and-easy-credit-card-theft.pdf

CSF Controls Related to Threats

HITRUST

CSF Controls Related to Threats

CSF Control for FastPOS (Exfiltration Methods)

- **Control Reference: 01.i Policy on the Use of Network Services**
  - **Control Text:** Users shall only be provided access to internal and external network services that they have been specifically authorized to use. Authentication and authorization mechanisms shall be applied to users and equipment.
  - **Implementation Requirement:** The organization shall specify the networks and network services to which users are authorized access.

CSF Controls Related to Threats

CSF Control for Top Emerging Malware

- **Control Reference: 09.j Controls Against Malicious Code**
  - **Control Text:** Detection, prevention, and recovery controls shall be implemented to protect against malicious code, and appropriate user awareness procedures on malicious code shall be provided.
  - **Implementation Requirement:** Protection against malicious code shall be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls.

CSF Controls Related to Threats

CSF Control for FastPOS (keylogger)

- **Control Reference: *10.h Control of operational software**
  - **Control Text:** There shall be procedures in place to control the installation of software on operational systems
  - **Implementation Requirement:** The organization shall maintain information systems according to a current baseline configuration and configure system security parameters to prevent misuse.

CSF Controls Related to Threats

CSF Control for Vulnerability Patching

- **Control Reference: *10.m Control of technical vulnerabilities**
  - **Control Text:** Timely information about technical vulnerabilities of systems being used shall be obtained; the organization's exposure to such vulnerabilities evaluated; and appropriate measures taken to address the associated risk
  - **Implementation Requirement:** Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within Appropriate, timely action shall be taken in response to the identification of potential technical vulnerabilities. Once a potential technical vulnerability has been identified, the organization shall identify the associated risks and the actions to be taken. Such action shall involve patching of vulnerable systems and/or applying other controls.

QUESTIONS?

HITRUST

Health Information Trust Alliance

Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight