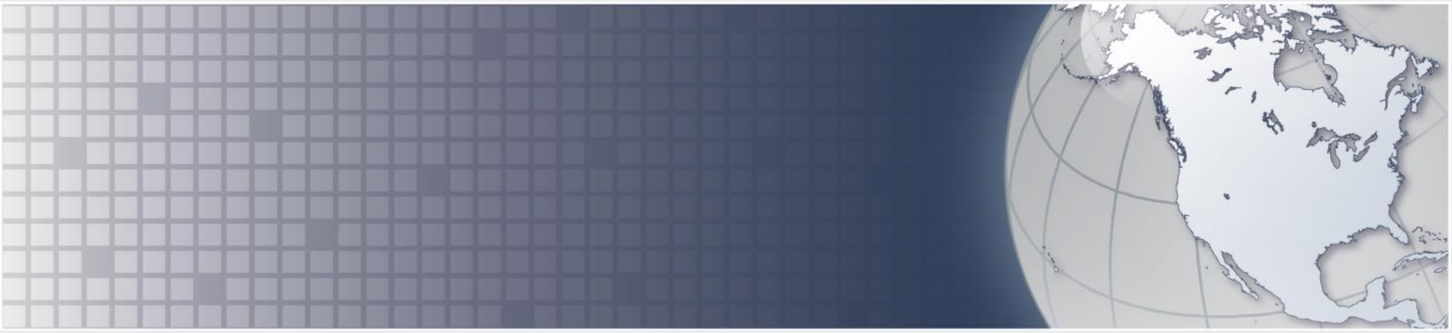
INTELLIGENCE ASSESSMENT



(U//FOUO) Increasing Use of Ransomware May Threaten US Civilian Government and Critical Infrastructure Networks

25 August 2016

Homeland Security

National Cyber-Forensics & Training Alliance

NCFTA

Office of Intelligence and Analysis
IA-0199-16

(U) Warning: *This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS*

(U) All US person information has been minimized. Should you require the minimized US person information, please contact the I&A Production Branch at IA.PM@hq.dhs.gov, IA.PM@dhs.sgov.gov, or IA.PM@dhs.ic.gov.

Homeland Security
Office of Intelligence and Analysis
National Cyber-Forensics & Training Alliance
INTELLIGENCE ASSESSMENT
25 August 2016

(U//FOUO) Increasing Use of Ransomware May Threaten US Civilian Government and Critical Infrastructure Networks

(U//FOUO) Prepared by the Office of Intelligence and Analysis (I&A). Coordinated with the National Cyber-Forensics and Training Alliance (NCFTA).

(U) Scope

(U//FOUO) This *Assessment* builds upon previous DHS assessments on ransomware threats to US government and civilian networks, including emergency services sector networks. The most recent assessment published on ransomware threats was issued in May 2015. The purpose of this *Assessment* is to provide federal, state, local, tribal, and private sector stakeholders awareness of potential cyber threats to US government and civilian networks to help them identify threats and design countermeasures to protect against future cyber operations. This *Assessment* is based on DHS fusion center data and a review of cybersecurity reporting on ransomware attacks against US networks across multiple sectors between January 2015 and June 2016. The information cutoff date is 29 June 2016.

(U) Key Judgments

(U//FOUO) I&A assesses ransomware campaigns are spreading rapidly as a result of widely available access to ransomware or its source code in underground markets and media reports on ransomware profits, increasingly threatening US government and civilian systems, especially those that enable critical services and key resources, by denying legitimate users access to their data.

(U//FOUO) I&A assesses new ransomware variants display increasingly advanced functions and capabilities, such as targeted delivery techniques, obfuscation mechanisms, persistence capabilities, and backup system deletion tools that constitute a high threat to US networks.

(U//FOUO) I&A assesses cybercriminals since at least the spring of 2016 have been using a variety of increasingly sophisticated mechanisms to distribute ransomware more effectively than they had in the past, such as advanced phishing campaigns using spoofed e-mail addresses and content, water-holing techniques, system vulnerability exploitation, and well-established botnet infrastructures.

(U//FOUO) I&A assesses non-traditional ransomware users, such as criminal hackers or state-sponsored cyber actors, may use ransomware variants as a means to obtain and maintain persistent illicit access to targeted networks not only to facilitate denial and destruction of data, but also as a distraction to obfuscate other types of fraudulent activity and cyber espionage.

(U//FOUO) Overview of Ransomware Campaigns

(U//FOUO) The term "ransomware campaigns" refers to all ransomware families, including variants and versions that share the capability to deny compromised victims access to critical data. Ransomware was initially observed in 1989 but generally was not regarded as pervasive and destructive until ransomware families such as CryptoWall and CrytpoLocker emerged in 2013 and demonstrated their abilities to quickly proliferate by using established botnets and exploit kits. Since then, ransomware has developed new capabilities, including payment forms, increasing encryption strength, and new delivery and distribution methods. More recently, high-profile media coverage of ransomware profits further fueled demand for new ransomware tools and services in underground cyber markets, leading to significant proliferation of additional variants between mid-2015 to early 2016.[1]

(U//FOUO) Ransomware Growth and Maturity Brings New Threats

(U//FOUO) I&A assesses the overall use of ransomware campaigns is spreading rapidly as a result of widely available access to ransomware in underground markets and media reports on ransomware profits, increasingly threatening US government and civilian systems, especially those that enable critical services and key resources, by denying legitimate users access to their data. Cyber actors since at least 2013 have deployed data-encrypting ransomware indiscriminately against US businesses, universities, maritime vessels, healthcare providers, emergency services providers, and SLTT governments to deny access to data until ransom demands have been met. These schemes in 2015 generated more than $24 million in illicit revenue, typically in bitcoin, according to a news article citing the FBI.[2] Ransomware campaigns experienced significant growth and increasing maturity in the past year as a result of the release of multiple ransomware variants in underground cyber markets, increased media coverage of ransomware campaign profits, and strong supply and demand in underground cyber markets.

» (U//FOUO) The number of ransomware variants released on underground markets nearly doubled in mid-2015, according to open source reports and other data received by the National Computer Emergency Response Team in the United Kingdom, also known as CERT-UK.[3] The surge in ransomware variants coincided with increased media coverage of ransomware profits, according to a CERT-UK assessment.[4]

» (U//FOUO) Additionally, ransomware source code was released in the underground cyber market between late 2015 and early 2016, enabling the development of customization features and allowing cyber actors to modify and make improvements to the malware. For example, a cyber actor using the nickname "RADAMANT" in January 2016 advertised the sale of RADAMANT ransomware malware source code in the Russian underground criminal forum exploit.in, according to a collaborative FBI source with excellent access, some of whose reporting has been corroborated in the past year.[5] The same actor initially advertised the RADAMANT kit for rent in December 2015 in the same forum, offered technical support, and secured hosting services, according to the same source.

(U//FOUO) New Variants Display Increasingly Advanced Functions and Capabilities

(U//FOUO) I&A assesses new ransomware variants display increasingly advanced functions and capabilities—such as targeted delivery techniques, obfuscation mechanisms, persistence capabilities, and backup system deletion tools—that constitute a high threat to US networks. For example, the ransomware Locky is deployed in a multi-stage, targeted fashion against vulnerable systems and can locate and delete backup systems, according to reports from DoD and DHS officials that we deem reliable based on their direct access and ability to analyze malware samples.[6] These capabilities could enable some cyber actors to improve their targeting techniques to identify and compromise systems lacking data backups and redundancy measures.

» (U//FOUO) Cyber actors in March 2016 targeted DoD and US federal civilian government webmail users with a ransomware campaign that used spoofed e-mail addresses to deliver the Locky variant, indicating a more focused targeting pattern than earlier versions of the malware, according to DHS and DoD technical reporting.[7,8] The malware employed a multi-stage payload delivery system that loads itself into a computer's memory before establishing an illicit and persistent access and encrypting files and documents, renaming file extensions, and deleting shadow snapshots that can prevent legitimate users' ability to recover affected files. This campaign distinguishes itself from previous campaigns by displaying an enhanced targeting capability and sophisticated obfuscation and evasion techniques, according to the same source.[9,10] Additionally, the malware featured functions that allowed cyber actors to conduct network reconnaissance, identify shared files and network drives, and locate and delete backup systems, indicating a significant progression in overall ransomware capabilities, according to the same source. [11,12]

» (U//FOUO) A ransomware attack in March 2016 compromised a US-based hospital using an outdated server vulnerability, according to a state government official with direct access to the information. The cyber actors used administrator-level access to locate and encrypt more than100,000 files on 4,000 systems, including 600 servers. This attack denied hospital personnel access to sensitive files for two days, according to the same reporting.[13]

» (U//FOUO) Cybersecurity officials in April discovered two Massachusetts government desktop computers infected with Locky ransomware, which encrypted three agency shared drives, according to DHS information obtained from a public sector cybersecurity official with direct and indirect access to the information through official duties.[14] Officials suggest this was a targeted campaign, as the commonwealth received 71 e-mails containing Locky-associated attachments over the course of a few hours, according to the same DHS information.[15] Unlike previous ransomware attacks that sporadically and indiscriminately targeted victims, this attack was deployed against users within the same organization in a short period of time, indicating a more focused targeting campaign.

(U//FOUO) Diversification of Distribution Mechanisms Increases Effective Deliveries

(U//FOUO) I&A assesses cybercriminals since at least the spring of 2016 have been using a variety of increasingly sophisticated mechanisms to distribute ransomware more effectively than they had in the past, such as advanced phishing campaigns using spoofed e-mail addresses and content, water-holing techniques, system vulnerability exploitation, and well established botnet infrastructures. Cyber actors traditionally leveraged e-mail spamming services and social engineering techniques to distribute ransomware sporadically and indiscriminately against an array of targets. Although these techniques are still being used, during the past two years we have observed a trend of more focused, refined campaigns that are likely to increase the successful infection and deployment against organizations that rely on computer systems to deliver critical services and key resources.

» (U//FOUO) Unknown cyber actors continue to use traditional social engineering tactics and phishing campaigns to deliver malicious attachments with embedded ransomware, although since spring 2016 we have observed increasingly focused, targeted campaigns. Once users clicked on the malicious attachment, the ransomware downloaded and executed, often along with legitimate processes, to compromise the targeted network. This technique was used to target private sector organizations as well as DoD and other US government e-mail users. For example, state and federal government employees in March 2016 received phishing e-mails that were spoofed to appear to originate from the user's network and contained malicious attachments with embedded first-stage malware that communicated with command-and-control infrastructure to obtain second-stage malware, likely ransomware, according to defense reporting.[16]

» (U//FOUO) Unknown cyber actors since at least July 2015 have used legitimate websites to host ransomware variants and infect visiting users, a technique known as water-holing. For example, unknown cyber actors in July 2015 used this technique to infect several New Mexico city government systems with Cryptowall 3.0 malware. The attackers planted a JavaScript exploit on a US website to deliver Cryptowall to users visiting a watering hole, targeting only those that were running Internet Explorer web browsers, according to a government official with firsthand access to the information through the course of normal duties.[17] Cryptolocker malware embedded on a legitimate site in April 2016 also was used to infect a computer server belonging to a US healthcare provider in Texas that resulted in the encryption of patient information, including medical history and insurance records, after a receptionist accessed the website for a nearby school district, according to an FBI source with excellent access.[18]

» (U//FOUO) Unknown cyber actors since 2014 have used access to well-established botnets to propagate ransomware, enhancing the overall success of malware delivery through automation and scalability. For example, communication infrastructure analysis indicates unknown cyber actors have used malware to distribute Locky and Crytpowall variants, respectively, according to analysis by a well-known cybersecurity firm.[19,20] Furthermore, Locky ransomware phishing e-mails strongly resembled those used in other campaigns, according to the same cybersecurity firm analysis.[21,22]

» (U//FOUO) Unknown cyber actors in 2016 also exploited unpatched system vulnerabilities to deliver ransomware and gain access to targeted networks. For example, unknown cyber actors in April 2016 conducted a ransomware attack against a US utility company by exploiting an outdated JBoss server that was running as a domain administrator, resulting in the encryption of the company's corporate file systems, according to FBI reporting obtained from an officer of another law enforcement agency.[23] The same server vulnerability was exploited to compromise the aforementioned US-based hospital network in March 2016, according to DHS officials with excellent access.

(U) Outlook and Implications

(U//FOUO) I&A assesses non-traditional ransomware users, such as state-sponsored cyber actors or criminal hackers, may use ransomware variants to obtain and maintain persistent illicit access to targeted networks not only as a means to facilitate denial and destruction of data, but also as a distraction to obfuscate other types of fraudulent activity as well. We expect ransomware attacks against US government and private sector networks to continue and likely increase as ransomware variants become even more stealthy, customizable, and accessible. Furthermore, recent advancements in ransomware functions and capabilities may provide an opportunity for non-traditional ransomware users to use in future computer network operations.

- (U//FOUO) Criminal hacker organizations such as the Syrian Electronic Army and Al-Qassam Cyber Fighters targeted Internet service providers and US financial sector entities in September 2012 and August 2013, respectively, with distributed denial-of-service attacks and website defacements in protests to political developments, according to open source reporting.[24] Although we have not seen these groups use ransomware to conduct attacks, we assess that currently available ransomware has the capability to deny the use of data and achieve the same objectives.

- (U//FOUO) Additionally, we assess that financially motivated, organized cybercriminal syndicates may use ransomware as a diversion tactic to facilitate other malware activity, such as data deletion and cyber espionage. Financially motivated cyber actors since at least 2012 have used DDoS attacks to distract some US banks from identifying and preventing fraudulent cash transfers, according to analysis by a well-known cybersecurity firm.[25] This technique was also used against other global targets. For example, the Blackenergy DDoS botnet in November 2012 was used to target a Brazilian bank to distract bank employees from identifying fraudulent activities, according to the same company.[26] To date, we have not seen evidence of cyber actors using ransomware as a distraction mechanism to facilitate other types of activity; however, new ransomware variants display the functionality and capability that could be used to generate the same effect.

(U) Mitigation, Prevention, and Response

- (U) Ensure anti-virus software is up-to-date and enable automated patches for your operating system and web browser.

- (U) Implement data backup and recovery plans and ensure they are not accessible from local networks. Conduct regular backups, test backup recovery on a regular basis, and store your critical data offline. Proper backups enable the victim to wipe their computer of every file and restore clean copies from the backups.

- (U) Only download software from trusted sites.

- (U) Do not open attachments or click on URLs in unsolicited e-mails or from untrusted sources. Access the URL by navigating through an organization's website directly.

- (U) If you become a victim of ransomware, before even considering paying, note that there have been instances in which an individual security researcher or company has developed decryption tools to unlock encrypted files. These are usually free or cost less than the ransom. The most challenging element is awareness that a decryptor may be available. Contact Law Enforcement if you become the victim of ransomware.

- (U) A Google doc that documents information about ransomware (including if a decryptor exists) is available by going to: https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml.

- (U) For more information, please visit: https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise.

(U) The following chart depicts some of the more common variants of ransomware and key attributes.[27]

(U) Sampling of Ransomware Variants

	Cryptolocker	**Locky**	**TeslaCrypt**	**Petya**	**SAMAS**	**Rokku**	**Keranger**	**Kimcil**
Encryption Algorithm	AES RSA-2048	AES-256 RSA-2048	AES-256	Salsa20	AES-256	Salsa20	AES and RSA Public Key	Rijndael block cipher
What is Encrypted/# of File Types	Encrypts non-.exe Files	Files Bitcoin Wallet Unmapped network shares	Files	Entire Hard Drive (Master Boot Record and Master File Table)	Network Encryption Files	Local Disks Network Shares	Everything in home directory and other file types	Web Servers
Is a Decryptor Available?	Yes	No (but one is available for a variation called AutoLocky)	Yes	Yes	No	No	Yes	Yes
Who are the Primary Targets?	No Specific Target	No Specific Target	Gaming	HR Departments	Healthcare	No Specific Target	BitTorrent Users	Magento eCommerce Customers
Initially Affected Region	Not Specified	United States	United States	North America	North America	Not Specified	North America	Not Specified
OS/Platform Affected	Windows	Windows	Windows	Windows	Windows	Windows	OS X	Windows
Accepted Payments	Bitcoin MoneyPak Paysafecard CashU Ukash	Bitcoin	Bitcoin MoneyPak Paysafecard Ukash	Bitcoin	Bitcoin	Bitcoin QR Code	Bitcoin Moneypack Ukash PaySafeCard	Bitcoin
How is it delivered?	Targeted Email	Spam Previous Botnet Infections (similar to DRIDEX)	Spam	Job Application	Various Exploits Found Via Jexboss	Spam	Fake BitTorrent client	Magneto Exploit

(U) Source Summary Statement

(U//FOUO) This Assessment is based on open sources, third-party trusted vendors, US government reports, and private industry reporting provided by the National Cyber Forensics and Training Alliance. The open source reporting indicates a wide range of cybersecurity reporting, some of which is obtained through various means, including technical analysis. We have ***high confidence*** *in our assessments due to government reporting that is obtained through sources that have direct access to the collected information. We deem this access as sufficient to corroborate the information obtained from open sources and third party trusted vendors.*

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

(U) Tracked by: HSEC-1.1, HSEC-1.2, HSEC-1.8

[1] (U); Isight; Intel-1288874; 24 NOV 2014; DOI UNK; (U); Overview of Ransomware History and Current Trends; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[2] (U); Harriet Taylor; CNBC; "Ransomware: Lucrative, fast growing, hard to stop"; 11 APR 2016; www.cnbc.com/2016/04/11/ransomware-lucrative-fast-growing-hard-to-stop.html; accessed on 29 JUL 2016.

[3] (U//FOUO); UK-CERT; CUK-27-05-16-CD; DOI UNK; (U//FOUO); Is Ransomware Still a Threat?; Extracted information is U//FOUO; Overall document classification is U//FOUO.

[4] (U//FOUO); UK-CERT; CUK-27-05-16-CD; DOI UNK; (U//FOUO); Is Ransomware Still a Threat?; Extracted information is U//FOUO; Overall document classification is U//FOUO.

[5] (U//FOUO); FBI; IIR 4 213 2429 16; 281456Z JAN 16; DOI JAN 2016; (U//FOUO); Announcement of the Sale of the Source Code for the Radamant Kit by a Cyber Actor Using the Moniker "RADAMANT" on The Online Forum Exploit.in, As of January 2016; Extracted information is U//FOUO; Overall document classification is U//FOUO.

[6] (U//FOUO); DoD; U//OO/132909-16; DOI UNK; (U//FOUO); Ransomware; Locky Placemat; Extracted information is U//FOUO; Overall document classification is U//FOUO.

[7] (U//FOUO); DoD; U//OO/132909-16; DOI UNK; (U//FOUO); Ransomware; Locky Placemat; Extracted information is U//FOUO; Overall document classification is U//FOUO.

[8] (U); Isight; 16-00002390; 25 FEB 2016; DOI UNK; (U) Locky: Malware Behavior, Capabilities, and Communications; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[9] (U//FOUO); DoD; U//OO/132909-16; DOI UNK; (U//FOUO); Ransomware; Locky Placemat; Extracted information is U//FOUO; Overall document classification is U//FOUO.

[10] (U); Isight; 16-00002390; 25 FEB 2016; DOI UNK; (U); Locky: Malware Behavior, Capabilities, and Communications; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[11] (U//FOUO); DoD; U//OO/132909-16; DOI UNK; (U//FOUO); Ransomware; Locky Placemat; Extracted information is U//FOUO; Overall document classification is U//FOUO.

[12] (U); Isight; 16-00002390; 25 FEB 2016; DOI UNK; (U); Locky: Malware Behavior, Capabilities, and Communications; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[13] (U//FOUO); DHS; IIR 4 044 0044 16; 190218Z MAY 2016; DOI 20 - 22 MAR 2016; (U//FOUO); Ransomware Infecting a US-Based Hospital via an Internet Protocol Address Resolving to Russia; Extracted information is U//FOUO; Overall document classification is U//FOUO.

[14] (U//FOUO); DHS; IIR 4 045 0191 16; 250234Z MAY 16; DOI APR 2016; (U//FOUO); Technical Details of Successful Locky Ransomware Infection on Commonwealth of Massachusetts Government Network; Extracted information is U//FOUO; Overall document classification is U//FOUO.

[15] (U//FOUO); DHS; IIR 4 045 0191 16; 250234Z MAY 16; DOI APR 2016; (U//FOUO); Technical Details of Successful Locky Ransomware Infection on Commonwealth of Massachusetts Government Network; Extracted information is U//FOUO; Overall document classification is U//FOUO.

[16] (U//FOUO); DoD; 132221-16; 311543Z MAR 2016; DOI MAR 2016; (U//FOUO); US Government Email Users Receive Phishing Emails with Malicious Attachments, March 2018; Extracted information is U//FOUO; Overall document classification is higher than U//FOUO.

[17] (U//FOUO); DHS; IIR 4 017 0027 16; 251920Z APR 2016; DOI 05 – 11 JUL 2015; (U//FOUO); Cryptowall 3.0 Ransomware Infected Local New Mexico Government and Banking Networks; Extracted information is U//FOUO; Overall document classification is U//FOUO.

[18] (U//FOUO); FBI; IIR 4 213 4695 16; 111539Z MAY 16; DOI APR 2016; (U//FOUO); Infection of a US Health Care Provider by Cryptolocker RSA 4096 Ransomware, As of April 2016; Extracted information is U//FOUO; Overall document classification is U//FOUO.

[19] (U); Isight; 16-00002390; 25 FEB 2016; DOI UNK; (U); Locky: Malware Behavior, Capabilities, and Communications; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[20] (U); Isight; Intel-1212922; 11 AUG 2014; DOI UNK; (U); Infrastructure Activity Suggests CryptoLocker Operators Preparing to Resume Distribution and Use; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[21] (U); Isight; 16-00002390; 25 FEB 2016; DOI UNK; (U); Locky: Malware Behavior, Capabilities, and Communications; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[22] (U); Isight; Intel-1212922; 11 AUG 2014; DOI UNK; (U); Infrastructure Activity Suggests CryptoLocker Operators Preparing to Resume Distribution and Use; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[23] (U//FOUO); FBI: IIR 4 213 4639 16; 051917Z MAY 2016; DOI APR 2016; (U//FOUO); Increase of Ransom Demand by Unidentified Cyber Actors in Ransomware Negotiations With an Identified US Utility Company, As of Late April 2016; Extracted information is U//FOUO; Overall document classification is U//FOUO.

[24] (U); Isight; Intel-937437; 13 SEP 2013; DOI UNK; (U); One Year Review and Look Forward: Option Ababil DDOS Campaign Against the US Financial Sector; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[25] (U); Isight; Intel-740500; 05 FEB 2013; DOI UNK; (U); DDOS Attacks Intended to Distract Banks from Cash-Outs Likely to Continue, Posing Threat to Much of the US Financial Sector; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[26] (U); Isight; Intel-690996; 13 NOV 2012; DOI UNK; (U); Blackenergy DDOS on Brazil's Itau Bank Possibly Meant to Divert Employee's Attention from Fraudulent Transactions; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[27] (U); National Cyber Forensics and Training Alliance; NCFTA's Malware and Cyber Threats Program Operations 18 AUG 2016; DOI 2016; (U); Common Malware Variants and Key Attributes; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Increasing Use of Ransomware May Threaten US Civilian Government and Critical Infrastructur

1. Please select partner type: Select One **and function:** Select One

2. What is the highest level of intelligence information that you receive? Select One

3. Please complete the following sentence: "I focus most of my time on:" Select One

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? ***(Check all that apply.)***

- □ Drive planning and preparedness efforts, training, and/or emergency response operations
- □ Observe, identify, and/or disrupt threats
- □ Share with partners
- □ Allocate resources (e.g. equipment and personnel)
- □ Reprioritize organizational focus
- □ Author or adjust policies and guidelines
- □ Initiate a law enforcement investigation
- □ Initiate your own regional-specific analysis
- □ Initiate your own topic-specific analysis
- □ Develop long-term homeland security strategies
- □ Do not plan to use
- □ Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product? Select One

10. Would you be willing to participate in a follow-up conversation about your feedback? Yes

To help us understand more about your organization so we can better tailor future products, please provide:

Name:

Organization:

Contact Number:

Position:

State:

Email:

Submit Request

Privacy Act Statement