Federal Bureau of Investigation
Intelligence
Assessment
Department of Homeland Security

Intelligence Assessment

(U//FOUO) Potential Impacts of a Data-Destruction Malware Attack on a US Critical Infrastructure Company's Networks

13 December 2013

(U) Executive Summary

(U//FOUO) With the severity of data-destruction malware attacks in 2012, including attacks on Saudi Aramco, Qatari RasGas, and South Korean media and banking organizations, US companies must become prepared for the increasing possibility they could become victim to a cyber attack that could delete data from various enterprise components, or impact an organization's capability to perform daily operations. Data destruction attacks could have a damaging impact for companies and organizations with industrial control system (ICS)[a] assets and infrastructure. In the current cyber climate, the FBI speculates it is not a question of if a US company will experience an attempted data-destruction attack, but when and which company will fall victim.

(U//FOUO) In 2013, the FBI asked several private-sector critical-infrastructure companies what consequences a data-deletion cyber attack would have on their businesses. The anticipated effects were significant in terms of costs of recovery and reconstitution, lost income, and company reputation.

(U//FOUO) All participants agreed the implications were greatly dependant on a sufficient data backup plan that included offline or other unaffected backups of data. Loss of data may include customer information and their product requirements, which would further affect the company's ability to meet customer needs. The participants also suggested product prices would be affected, as well as competitive edge, and the long-term effects would include new regulations, enhanced cyber security and associated costs, environmental and litigation concerns. In addition to a successful data recovery, a solid public relations message would be critical to the targeted company's long-term survival. Participants were uncertain as to how the affected business could meet customer needs during the downtime, and whether the business would recover from any potential loss of business.

(U//FOUO) The possible shutdown of ICS networks was cautiously addressed by one participant. This participant believed that due to safety measures implemented for physical threats, such as natural disasters, the ICS would shut down in safe mode. If this were true, the physical safety consequences would be limited due to a lack of production or transport of product(s). However, the shutdown could have large-scale implications for power, utilities, energy, water, and other critical resources with dependencies tied to the company.

(U//FOUO) The Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has prepared specific guidance (included within this paper) on preparation and planning for such an event. Data protection, recovery and reconstitution plans, and computer network defense best practices should be implemented and continuously reviewed and validated in advance, in order to provide an organization with robust preparation, detection and containment strategies in the event a successful destructive malware attack were to occur.

[a] (U) Cyber terms are defined in Appendix D.

(U) Scope Note

(U//FOUO) This paper uses "What If" Analysis to speculate on the implications of data-destruction attacks against US critical-infrastructure companies. It is not an assessment of the likelihood of any future events. The analysis was undertaken under the direction of the FBI's Assistant Director for the Cyber Division after the cyber attack on Saudi Aramco in 2012. This is a baseline assessment.

(U//FOUO) The discussions with industry occurred in September 2013. Individuals from five critical infrastructure companies were involved, from C-level security officers to IT supervisors and analysts. The FBI presented the participants with a scenario indicating online computer data was destroyed and asked to speculate on business consequences. The FBI facilitators posed additional questions regarding continuity plans, disaster recovery, and IT readiness to help assess potential damage to each company at the time of the discussion.

(U//FOUO) This analysis mentions the destruction of ICS-network computer resources and it briefly discusses the consequences; however, as a deliberate attack against a control system has not occurred and most company representatives did not feel comfortable discussing possible outcomes, there was no data to contribute to any assessments on that subject.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) Source Summary Statement

(U//FOUO) Sources for estimates on damages to companies due to a data destruction malware attack were structured group discussions with company representatives. Reports from mostly reliable media organizations were used to provide background. Some open source reports were taken from more biased papers, but those concerns are addressed in this paper.

(U) Implications of Data Destruction Attack

(U//FOUO) In September 2013, the FBI asked several private-sector critical-infrastructure companies what the consequences of a data-destruction cyber attack would be on their business. In the scenario provided by the FBI, companies were asked to assume the data on most of their workstations and several central servers had been destroyed, and to anticipate what the effects of the data loss would be. Participant companies discussed several categories of implications: Recovery Efforts, Financial, Company Brand, Human Capital, Business Operations, and Critical Infrastructure Consequences.

(U) Recovery Efforts Dependant on Backups

(U//FOUO) All participants agreed the implications were greatly dependant on a sufficient data backup plan. Data recovery, if offline backups were available, could be time- and labor-intensive. The existence of offline backups was not guaranteed. Off-site, disk-based backups were prevalent, given expense and reliability concerns over tape backups. In the case of data destruction malware, however, there would be a strong possibility the off-site, network-connected backups would also be deleted. If unaffected backups were not available, recovery of data would not be possible without forensic tools, and only then if the entire drive had not been overwritten. To recover data forensically would most likely require hiring an outside firm, as well.

(U//FOUO) If centralized servers were not used for file storage, and workstations had their own data saved to their hard drives, this data would be lost, unless forensic software and personnel were able to recover the data, or clean backups were available.

(U//FOUO) If a company were able to restore data and had disk images to recover workstations, reinstalling disk images on workstations would be labor-intensive. If the images were not kept up-to-date with patching, recovering useable workstations would take exponentially longer. In addition, many employees use applications not found on the standard workstation image and this specialized software would be critical to full business performance.

(U//FOUO) Virtual servers were a concern, as the entirety of the data would be preserved on digital snapshots, and any malware present would be propagated to the restored server. To prevent a recurrence of the malware when restoring from backups, an analysis would be required to ensure the backups were clean before restoring the systems. This process would cause additional downtime. In addition, to perform the needed analysis, the response team would need to know the indicators of the infection, which may require waiting until the forensic analysis was completed, adding additional downtime.

(U//FOUO) Participants expressed concern for the availability of critical data and applications. Potential targets with high impact would include centralized storage devices (cloud computing servers, data warehouses and repositories) and network devices specifically relating to the loss of routing within an organization's network.

(U) Company Brand

(U//FOUO) Public reputation and trust would affect the stock value of publicly-traded companies. Given that Saudi Aramco, the company most affected by a previous data-destruction attack, is not publicly traded, no damage estimates can be determined.

(U//FOUO) If the company brand is tarnished by a severe cyber incident, future capital investments and capital partnership agreements may be limited by investors' sense of the reliability of the company. This would inhibit future business growth and competitive edge.

(U//FOUO) A solid public relations message would be critical to the targeted company's long term survival. While participants agreed this was critical and that such messaging could be prepared or carefully thought through in advance, many companies admitted their preparations for such a public relations problem were inadequate.

(U) Financial Impact

(U//FOUO) In addition to the financial impact of falling stock value, if the company engages in futures trading, that trading would be severely disrupted. Large manufacturing firms and other product providers would have their deliveries to customers delayed, further disrupting revenues from production and sales.

(U//FOUO) When discussing financial impact, companies were unable to provide concrete numbers, as the impact would depend on the size of the company—and their stock value—prior to the attack.

(U//FOUO) As companies make determinations for preventative measures, financial officers need to be consulted and given a full picture of the disruption. The company's individualized financial picture will help risk calculations.

(U) Human Capital

(U//FOUO) The employees would be affected as well. Psychological effects include employees' trust in the company, job security, and overall morale. During recovery, any employees whose work required functioning network and computer resources would need to be sent home. The company would need to make determinations about whether these employees would continue to be paid.

(U) Business Operations

(U//FOUO) Participants were uncertain how the business could meet customer needs during the downtime, and whether the business could recover from any potential loss of business. Loss of data may include customer information and product requirements which would further affect the company's ability to meet company needs. The participants suggested product prices would be affected, as well as competitive edge.

(U//FOUO) The participants felt the long-term effects would include new regulations, enhanced cyber security and associated costs, as well as environmental and litigation concerns. Whether the stocks, brand, and company reputation could recover would depend on the company's successful public relations management during the incident.

(U) Critical Infrastructure Consequences

(U//FOUO) The possible shutdown of ICS networks was cautiously addressed by one company. This company believed that due to safety measures against physical threats, such as natural disasters, the ICS would shut down in safe mode. While the physical safety consequences would be limited, due to a lack of production or transport of product(s), the shutdown could have large-scale implications for power, utilities, energy, water, and other critical resources with dependencies tied to the company.

(U) Is the Assumption of a Successful Recovery Overly Optimistic?

(U//FOUO) During the discussion, the companies generally assumed they would be able to recover through backup programs and a successful recovery method. However, they wondered whether it could have a more significant destructive impact: the failure of the company.

(U) Examples of Data-Destruction Attacks

(U) South Korean Media Companies—March 2013

(U) On 20 March 2013, the Korean Broadcasting Service and approximately six banking institutions were impacted by malware.

- (U) The malware used was different in code and function from the Shamoon malware, but recovery methods were similar. As with Shamoon, the malware used deleted just enough data to make the machines unusable. The malware was specifically written for Korean targets, and checked for Korean antivirus products to disable. The destructive malware attack on South Korean companies defaced the machines with a message from the "WhoIs Team."[1]

- (U//FOUO) FBI analysis determined the malware did not have the functionality to overwrite or forensically wipe the entire drive, but the malware will attempt to delete the contents. The data is recoverable, but remediation and recovery steps from an attack of the malware would require extensive effort to recover.[2]

(U) Saudi Aramco—August 2012

(U//FOUO) On 15 August 2012, a version of the malware called Shamoon was activated on Saudi Aramco's networks. The Shamoon virus is designed to overwrite user data and system data directories, then the disk's Master Boot Record (MBR) and Volume Boot Record (VBR), thus preventing the computer from rebooting. In the Saudi Aramco case, the Shamoon virus did not overwrite entire disks, but did overwrite enough data to prevent access to the affected file

systems. The malware operation also destroyed substantial file data; however, 2012 analysis by private researchers indicated some files were still intact and recoverable. [3]

(U) Qatar's RasGas—August 2012

(U//FOUO) On 30 August 2012, RasGas, the world's second largest producer of liquefied natural gas, publically stated that the company was facing technical issues after being infected by an unknown virus since 27 August 2012. [4] Some news reports indicated that the virus was Shamoon.[5] The Shamoon virus is designed to overwrite user data and system data directories and then the disk's MBR and Volume Boot Record VBR, thus preventing the computer from rebooting.[6]

(U) South Korean Jungang Daily Newspaper—June 2012

(U) In June 2012, two conservative Seoul newspapers, the *Jungang Ilbo* and the *Korean Jungang Daily*, fell victim to a Web site defacement and a data deletion of database servers holding the paper's news filing and production systems.[7] The English-language *Daily* stated that both papers lost databases for articles and photos, as well as their editing system, which disrupted production.[8]

(U) Iranian Oil and Shipping Companies—April 2012

(U//FOUO) On 23 April 2012, Iranian news agencies began publicly reporting the Iranian Oil Ministry and the National Iranian Oil Company (NIOC) had been the targets of a cyber attack. The initial reports indicated the virus unsuccessfully attempted to delete data from oil ministry servers, according to Open Source Center reporting.[9]

(U) South Korean Nonghyup Bank—April 2011

(U) In a data-destruction cyber attack that started on 12 April 2011, half of the 500-plus servers belonging to the National Agricultural Cooperative Federation (Nonghyup Bank) were crippled, including servers controlling ATMs, credit card access, and online banking. These functions were severely impaired for approximately one week, affecting roughly 30 million customers.[10] South Korean officials indicated, at the time, some of the data might never be recovered. The bank, with approximately 5,000 branches, struggled with more than 30,000 customer complaints and 1,000 compensation claims.[11]

(U) Outlook and Implications

(U//FOUO) If the speculated events in this analysis were to take place, there would likely be multiple impacts on the United States as a whole. New regulation and guidelines would most likely be released by the US Federal Government in an attempt to prevent more damage. The competitors within the affected sector would possibly see residual effects that could include increased profits or decreased customers/profits, depending on the trepidation experienced by the public. The government response would be extremely dependant on the actor attributed to the activity and whether ICS components were affected.

(U//FOUO) The FBI judges that going forward the use data destruction malware in times of conflict will be considered as a potential vector by many nation states and non-state actors. However, the actors willing to use data destruction malware in the current global political climate will remain limited.

(U) Preparation and Planning

(U) In the appendices, ICS-CERT provides planning and mitigation suggestions.

(U) Intelligence Collection Requirements Addressed in Paper/NIPF Requirements

(U/FOUO) This intelligence study addresses requirements contained in the FBI National Standing Collection Requirements WW-HSEC-WMD-SR-0004-13.I.B.1 contained in TIA2011A.I.A.4.1.

(U) This assessment was prepared by the Critical Infrastructure Cyber Intelligence Unit (CICIU) of the FBI and the Industrial Control System Cyber Emergency Response Team (ICS-CERT) of DHS. Comments and queries may be addressed to the CICIU Unit Chief at 703-633-4626 or ICS-CERT 877-776-7585.

(U) To inquire about additional mitigation support or to report an incident, please contact FBI or DHS at US Department of Homeland Security, National Cybersecurity and Communications Integration Center (NCCIC), NCCIC Duty Officer (NDO), 888-282-0870 / 703-235-8832, nccic@us-cert.gov. For more information, visit www.us-cert.gov or www.ics-cert.org.

(U) Appendix A: Preparation and Planning: Distribution Vectors

(U) It is important that an organization assess their environment for various channels from which destructive malware could potentially be mass delivered and/or propagate throughout the environment.

- (U) Enterprise Applications – particularly those which have the capability to directly interface with and impact multiple hosts and endpoints. Common examples include:
  - ✓ (U) Patch Management Systems
  - ✓ (U) Asset Management Systems
  - ✓ (U) Remote Assistance software (typically utilized by an enterprise Help Desk)
  - ✓ (U) Anti-Virus
  - ✓ (U) Systems assigned to system and network administrative personnel
  - ✓ (U) Centralized Backup Servers
  - ✓ (U) Centralized File Shares

(U) Appendix B: Preparation and Planning: Recovery and Reconstitution Planning

(U) A Business Impact Analysis (BIA)[12] is a key component of contingency planning and preparation. The overall output of a BIA will provide an organization with two key components (as related to critical mission/business operations):

- (U) Characterization and classification of system components
- (U) Interdependencies

(U) In order to adequately plan for a potentially destructive malware attack, an organization should address the availability and accessibility for the following resources (and should include the scope of these items within Incident Response exercises and scenarios):

- (U) Comprehensive inventory of all mission critical systems and applications
  - ✓ (U) Versioning information
  - ✓ (U) System / application dependencies
  - ✓ (U) System partitioning/ storage configuration and connectivity
  - ✓ (U) Asset Owners / Points of Contact
- (U) Comprehensive inventory of all mission critical systems and applications
  - ✓ (U) Versioning information
  - ✓ (U) System / application dependencies
  - ✓ (U) System partitioning/ storage configuration and connectivity
  - ✓ (U) Asset Owners / Points of Contact
- (U) Contact information for all essential personnel within the organization
- (U) Secure communications channel for recovery teams
- (U) Contact information for external organizational-dependant resources
  - ✓ (U) Communication Providers
  - ✓ (U) Vendors (hardware / software)
  - ✓ (U) Outreach partners / External Stakeholders
- (U) Service Contract Numbers - for engaging vendor support
- (U) Organizational Procurement Points of Contact
- (U) ISO / image files for baseline restoration of critical systems and applications
  - ✓ (U) Operating System installation media
  - ✓ (U) Service Packs / Patches
  - ✓ (U) Firmware
  - ✓ (U) Application software installation packages
- (U) Licensing/activation keys for Operating Systems (OS) and dependant applications
- (U) Enterprise Network Topology and Architecture diagrams
- (U) System and application documentation
- (U) Hard copies of operational checklists and playbooks
- (U) System and application configuration backup files
- (U) Data backup files (full/differential)
- (U) System and application security baseline and hardening checklists/guidelines
- (U) System and application integrity test and acceptance checklists

(U) Appendix C: Preparation and Planning: Best Practices and Recommended Strategies

(U) In addition to recovery and reconstitution planning, common strategies can be followed to strengthen an organization's resilience against destructive malware.

- (U) Communication Flow
  - ✓ (U) Ensure proper network segmentation[13]
  - ✓ (U) Ensure that network access-controls are formally defined, documented, and implemented
  - ✓ (U) Increase awareness of systems that can be utilized as a gateway (lateral movement) or can directly connect to additional endpoints throughout an enterprise
  - ✓ (U) Ensure that multiple layers of network access-controls exist for critical network segments
    - (U) Control system network
    - (U) Critical assets
    - (U) Database servers
    - (U) Data warehouses
- (U) Access Control
  - ✓ (U) Require two factor authentication for interactive logons
  - ✓ (U) Do not use privileged accounts for daily job functions (general internet browsing, reading and opening email messages and attachments)
  - ✓ (U) Formally authorize, document, and track accounts which have administrative capabilities throughout the enterprise
  - ✓ (U) Accounts which are utilized to authenticate to centralized enterprise application servers or devices should not contain elevated permissions on downstream systems and resources throughout the enterprise
  - ✓ (U) Utilize separate accounts for systems within segmented zones (ex: DMZ, control system network).
    - (U) Consider enforcing distinctive password policies for systems within separate zones (minimizing the risk of similar passwords being utilized across multiple zones and network segments)
- (U) Monitoring, Auditing, and Assessments
  - ✓ (U) Audit and review security logs for references to enterprise-level administrative (privileged) and service accounts
  - ✓ (U) Ensure proper monitoring and review of enterprise-based password policies and requirements.
    - (U) Ensure any changes to the policy are formally authorized, documented, and tracked.
  - ✓ (U) Validate that network devices log and audit all configuration changes
    - (U) Ensure that the scope of network device configuration modifications correlate to authorized and approved changes.
  - ✓ (U) Review network flow data for signs of anomalous activity
    - (U) Connections utilizing ports which do not correlate to the standard communication flow associated with an application
    - (U) Activity correlating to port scanning or enumeration
  - ✓ (U) For enterprise application components which have the capability to directly interface with multiple hosts and endpoints, ensure that enhanced auditing and monitoring controls are enforced
    - (U) Auditing and integrity validation of any files (ex: patches, signatures) which are deployed via a centralized component
    - (U) Continuous review of access attempts by specific accounts utilized as part of a centralized component
    - (U) Network flow monitoring, specifically for signs of unusual communication flows - as observed from a centralized application component
- (U) System and Application Hardening
  - ✓ (U) Perform frequent vulnerability assessments for systems within an enterprise
  - ✓ (U) Ensure patch management processes are formally defined and implemented
    - (U) Patch management should encompass not only operating system (OS) patches, but

patches for integrated applications and components

- (U) Thoroughly test and implement patches in a timely manner

✓ (U) Ensure that the underlying Operating System (OS) and dependencies (ex: IIS, Apache, SQL) supporting an application are configured and hardened based upon industry-standard best practice recommendations

✓ (U) Prevent end-user capabilities to bypass application-level security controls (ex: disabling Antivirus on a local workstation)

(U) Disable un-necessary or un-utilized features and/or services

(U) Appendix D: Terms

(U) ***Computer Network Operations (CNO)***: Comprised of computer network attack (CNA), computer network defense (CND), and/or computer network exploitation (CNE) activities.

- (U) ***CNA***: Actions taken through use of computer networks to disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computer or networks themselves.
- (U) ***CND***: Actions taken through use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activities within information systems and computer networks
- (U) ***CNE***: Unauthorized intrusions into networks for the purpose of viewing and collecting information or steal computer resources.

(U) ***Distributed Denial of Service (DDOS)***: An attacker uses malware on multiple computers to cause them to simultaneously attack a computer resource such as a Web site or IP address to prevent legitimate use of that

(U) ***Domain Name Servers (DNS)***: An internet service that translates domain names into IP addresses.

(U) Expression of data size: The unit byte is used for digital information. The term is used interchangeably whether talking about size in terms of Base 2 (binary) or Base 10 data sizes. The translated values are different, however.

- ***Gigabytes (GB)***: 1GB = 1,000,000,000 bytes
- ***Terabytes (TB)***: 1TB = 1,000,000,000,000 bytes = 1,000 GB

(U) ***Industrial Control System (ICS)***: A broad term for any kind of automated system that controls the functions of a physical process.

(U) ***Virtual Machine Snapshot***: Virtual machines are software-based emulations of what would normally be a hardware and software-based system. Virtual machines are normally backed-up in 'snapshots', which captures the entire software emulation in a single file.

(U) Endnotes

[1] (U) Online Publication; General Dynamics: *Fidelis Cybersecurity Solutions; Fidelis Threat Advisory #1008: Darkseoul/Jokra Analysis and Recovery*; 21 March 2013; accessed 7 June 2013; Source was the analysis of malware samples acquired by Fidelis.
[2] (U) NCIJTF; 26 March 2013; 20 March 2013; "(U//FOUO) NCIJTF Analysis of Cyber Attacks Against South Korean Banks and Broadcasting Stations"; UNCLASSIFIED//FOUO; UNCLASSIFIED//FOUO; Source is forensic analysis of malware.
[3] (U) Online Publication; General Dynamics: *Fidelis Cybersecurity Solutions; Fidelis Threat Advisory #1007: Recovering from Shamoon*; 1 November 2012; Source is the company's forensic analysis.
[4] (U) Online publication; Camilla Hall and Javier Blas; *The Financial Times*; "(U) Qatar group falls victim to virus attack"; 30 August 2102; accessed 7 June 2013; Source was a press release from RasGas.
[5] (U) Online Publication; Michael Harper; RedOrbit.com; "Energy Company RasGas is Infected With Shamoon Virus"; 31 August 2012; http://www.redorbit.com/news/technology/1112685657/shamoon-virus-rasgas-aramco-033112; Accessed 7 June 2013; Inaccessible underlying sources.
[6] (U) *Op. cit..*, endnote 3.
[7] (U) Online Publication; Associated Press; 16 January 2013; "North Korea Behind Cyberattack on Seoul Newspaper Joongang Iblo; www.news.com.au/world-news/n-korea-behind-cyberattack-on-seoul-newspaper-joongang-ilbo-south-korea/story-fndir2ev-1226555457472; accessed 30 September 2013.
[8] (U) Online Publication; AAP; 11 June 2012; "South Korean newspaper JoongAng Ilbo hit by major cyber attack"; www.news.com.au/breaking-news/world/south-korean-newspaper-joongang-ilbo-hit-by-major-cyber-attack/story-e6frfkui-1226391202749; accessed 30 September 2013.
[9] (U//FOUO) OSC; IAP20120423950060; "(U//FOUO) Iran Rejects Damage On Oil Ministry Data In Recent Cyber Attack"; UNCLASSIFIED//FOUO; UNCLASSIFIED//FOUO; Source is open source media.
[10] (U) Online Publication; Chico Harlan and Ellen Nakashima; *The Washington Post*; "Suspected North Korean cyberattack on a bank raises fears for S. Korea, allies"; 29 August 2011; www.articles.wp.com/2011-08-29/world/35271097_1_bank-incident-bank-attack-cyberattack; accessed on 6 December 2013; Sources include interviews and statements from South Korean officials and investigators and IT security specialists.
[11] (U) Online Publication; UPI; "South Korea blames North for cyberattack"; www.upi.com/Top_News/Special/2011/05/04/South-Korea-blames-North-Korea-for-cyberattack/UPI-59211304504280/#ixzz2gkdTxifL; 4 May 2011; Sources include a report and statements by officials in the Seoul Central Prosecutor's Office.
[12] (U) Online Publication; National Institute for Standards and Technology; http://web.nvd.nist.gov/view/ncp/repository; accessed 30 September 2013.
[13] (U) Online Publication; ICS-CERT; http://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf; accessed 30 September 2013.

Distribution

LEO
DSAC
Infragard
FBI Intranet
SIPRNet
JWICS
LNI
IC3
US-CERT