Homeland Security
Intelligence Enterprise
INTELLIGENCE NOTE
4 June 2018

(U) Cybersecurity

(U//FOUO) Unidentified Cyber Actor Attacks State and Local Government Networks with GrandCrab Ransomware

(U//FOUO) Scope. This *Intelligence Note* provides recent intelligence and indicators of compromise (IOCs) on a recent ransomware attack against state and local government agencies. I&A prepared this *Note* for federal civilian, state, and local government network defenders.

(U//FOUO) Prepared by the Office of Intelligence and Analysis (I&A), Cyber Mission Center. Coordinated with the National Cybersecurity and Communications Integration Center (NCCIC).

(U//FOUO) GrandCrab Ransomware Encrypts Municipality Servers, Destroys Data; Infects State Judicial Branch Computers

(U//FOUO) An unidentified cyber actor in mid-March 2018 used GrandCrab Version 2 ransomware to attack a State of Connecticut municipality network and a state judicial branch network, according to DHS reporting derived from a state law enforcement official with direct and indirect access.[1] The municipality did not pay the ransom, resulting in the encryption of multiple servers that affected some data backups and the loss of tax payment information and assessor data. The attack against the state judicial branch resulted in the infection of numerous computers, but minimal content encryption, according to the same DHS report.

(U//FOUO) The unidentified cyber actor introduced the ransomware used against the judicial branch network through a vendor server/host; the ransomware then harvested cached credentials of high-level privileged accounts, according to the same DHS report. The actor then used the credentials to access two servers on the network and propagate the malware via server message block (SMB).[a] Connecticut state cybersecurity officials were able to block the ransomware's communication with external infrastructure, which prevented the encryption of additional hosts and data loss, according to the same DHS report.

(U) GandCrab Malware

(U) Released in late January 2018, GandCrab, also called "GrandCrab," is a ransomware variant distributed by exploit kits that requires communication with the ransomware's command-and-control (C2) server to encrypt files of an infected computer, according to an online technical support site.[2] The developers of GandCrab recently upgraded the original version after Romanian police and BitDefender mitigated infections by recovering its decryption keys, according to a separate article from the same online technical support site. As of 6 March 2018, no free decryption key is available to victims of GandCrab version 2.[3] GandCrab uses NameCoin's .BIT as its top-level domain (TLD); therefore, variants of the ransomware using the .BIT TLD must also use a domain name server that supports .BIT, according to the same online technical support site. Upon infection, GandCrab will attempt to query the ransomware's C2 servers on the .BIT domain to establish communication. GandCrab will not encrypt a host's content with the .CRAB extension if communication is not established with the C2 server, according to the same online technical support site.

[a] (U) SMB is a network file-sharing protocol.

(U) Support to Computer Network Defense

(U//FOUO) Connecticut cybersecurity officials associated the following IOCs with the GrandCrab version 2 infections, according to the same DHS report.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Element	Value
GrandCrab, Version 2 DNS Servers	79.137.133.151, 109.234.35.56.
File Name / MD5 Hash	gchtdu.exe / 56e3369852740a95236d6fcf9112b0c3
File Name / MD5 Hash	rund11.exe / 77c719768edd5f2b59add43661c41b9e
File Name / MD5 Hash	xmqjzi.exe / 897b61e6cf71edc8365aed32f6c4c372
File Name / MD5 Hash	itgkkl.exe / 85d31696c153d9c3bfb00e09649bb7a9
File Name / MD5 Hash	default.exe / 8d7a6ecb9a140a735fc607db026d59ce

(U//FOUO) The following IOCs are also associated with GrandCrab Version 2, according to two technical support sites.[4,5,6]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Element	Value
IP Address	185.70.186.150
Hash	966a0852c8adbea0b7b7aada7c2c851ee642c7bca7da3b29ee143f47ddeb90a5
MD5 Hash	be7b200d2115663a391c7f832559b461
SHA-1 Hash	d68ae25b3429e07ac370ded2f0514b8219fc1174
Authentihash	4066a78182b4922aa502818a0f5e65392ff2a70ad34a22a455923590b2ce00c
Imphash	7b6dd4245c054681d7b6b1f9b76fe984
File Type	Win32.exe
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
SSDeep	1536:BLT40re0mkSRJGglKtjzcqvsWjcdHzUaDFIMDM3tOo4xgvz2pvhWuEXjNF9RfO0:bo0RmkS2SqQHNgtf4xlz2pJhEnP20
TRiD	Win32 Executable MS Visual C++ (generic) (41%) Win64 Executable (generic) (36.3%) Win32 Dynamic Link Library (generic) (8.6%) Win 32 Executable (generic) (5.9%) OS/2 Executable (generic) (2.6%)
File Size	134 KB

(U) Reporting Computer Security Incidents
(U) To report a computer security incident, either contact NCCIC 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//FOUO); DHS; IIR 4 007 0381 18; 241632Z APR 18; DOI 09-10 MAR 2018; (U//FOUO); IIR 4 007 0381 18/CT - GrandCrab Ransomware, Version 2 Attack Against Connecticut State and Local Government Agencies; Extracted information is U//FOUO; Overall document classification is U//FOUO.

[2] (U); BleepingComputer; "GandCrab Ransomware Distributed by Exploit Kits; Appends GDCB Extension"; 29 JAN 2018; https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-distributed-by-exploit-kits-appends-gdcb-extension/; Accessed on 30 APR 2018.

[3] (U); BleepingComputer; "GandCrab Ransomware Distributed by Exploit Kits; Appends GDCB Extension"; 29 JAN 2018; https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-distributed-by-exploit-kits-appends-gdcb-extension/; Accessed on 30 APR 2018.

[4] (U); BleepingComputer; "GandCrab Ransomware Version 2 Released With New .Crab Extension & Other Changes"; 06 MAR 2018; https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-version-2-released-with-new-crab-extension-and-other-changes/; Accessed on 30 APR 2018.

[5] (U); VirusTotal; "details"; 30 APR 2018; https://www.virustotal.com/#/file/966a0852c8adbea0b7b7aada7c2c851ee642c7bca7da3b29ee143f47ddeb90a5/details; Accessed on 21 MAY 2018.

[6] (U); VirusTotal; "relations"; 30 APR 2018; https://www.virustotal.com/#/file/966a0852c8adbea0b7b7aada7c2c851ee642c7bca7da3b29ee143f47ddeb90a5/relations; Accessed on 21 MAY 2018.