CERT Australia | 2013-71

New Ransomware campaign

Abstract	CERT Australia has received a number of reports regarding a new ransomware campaign targeting end-users. Ransomware is a type of software which restricts access to a victim computer system, and demands a ransom be paid to the perpetrator in order for the restriction to be removed. This publication is provided to warn partners of this activity and assist those affected in detecting and mitigating malicious activity.

Background

CERT Australia has received a number of reports from victims of a new ransomware campaign targeting end-user systems. The malicious software is commonly known by the name *CryptoLocker*.

Ransomware is a type of software which restricts access to a victim computer system, and demands a ransom be paid to the perpetrator in order for the restriction to be removed.

Details

As with other ransomware variants, *CryptoLocker* encrypts documents, photos, databases and certificate files, and then demands payment of an amount in the vicinity of $300. In the case of this malware, the files are encrypted using public key cryptography, so the key is never stored on the machine, and thus is not available for acquisition using file recovery or other forensic techniques.

Of particular note, the *CryptoLocker* ransomware searches connected network shares for the specified document types, and thus will encrypt any backups that are reachable via mounted network drives. In previous ransomware campaigns CERT Australia was contacted by a number of organisations that had suffered significant business disruption as a result of corrupted backups.

In order to reduce attractiveness of the ransomware business model, CERT Australia recommends against payment of any amounts demanded by the operators of this type of malicious software.

Files with the extensions listed below are targeted by current versions of the *CryptoLocker* ransomware:

.3fr, .accdb, .ai, .arw, .bay, .cdr, .cer, .cr2, .crt, .crw, .dbf, .dcr, .der, .dng, .doc, .docm, .docx, .dwg, .dxf, .dxg, .eps, .erf, .indd, .jpe, .jpg, .kdc, .mdb, .mdf, .mef, .mrw, .nef, .nrw, .odb, .odm, .odp, .ods, .odt, .orf, .p12, .p7b, .p7c, .pdd, .pef, .pem, .pfx, .ppt, .pptm, .pptx, .psd, .pst, .ptx, .r3d, .raf, .raw, .rtf, .rw2, .rwl, .srf, .srw, .wb2, .wpd, .wps, .xlk, .xls, .xlsb, .xlsm, .xlsx

A list of the files on a particular machine that have been encrypted by the malware are available at the following Windows registry key:

HK_CURRENT_USER\Software*CryptoLocker*\Files

Current reporting indicates the majority of incidents involve the user opening a malicious email attachment containing the *CryptoLocker* malware, or visiting a website which exploits an application running on the user's PC to install the ransomware.

Please see links included below for additional analysis and information.[1]

Specific recommendations

CERT Australia suggests partners consider the following specific mitigations to protect against this cyber security risk:

- Activate Volume Shadow Copy on the relevant Windows PCs. This feature maintains previous versions of files in a location that is not accessible by current samples of *CryptoLocker*. Once the malware has been removed from an infected PC, files mirrored by the Volume Shadow Copy service can be recovered by the user.
- Make regular backups of valuable files and maintain an offline copy. As online drives and network shares are encrypted by the malware any connected backups will be rendered unusable.
- Ensure computer systems are running antivirus software with the latest antivirus signatures.
- Consider implementing application whitelisting or, at least, software restriction policies to hinder the ability of malicious software to execute successfully. [2]

General recommendations

CERT Australia suggests partners consider the following general mitigations to protect against this and other cyber security risks:

- Use application white-listing to only allow specifically authorised applications to operate on networks. This mitigation helps prevent malicious software or unauthorised applications from executing.
- Ensure applications and operating systems are kept up-to-date with the latest software patches.
- Ensure users are restricted from, or are administratively prohibited from installing unauthorised software and browsing the internet with administrator privileges.
- Remove, disable, or rename any default system accounts wherever possible.
- Enforce strong passphrase policies to reduce the risk from brute forcing attempts.
- Implement account lockout policies to reduce the risk from brute forcing attempts.
- Monitor the creation of administrator level accounts by third-party vendors.

- Monitor intrusion detection and/or prevention systems, user logs and server logs for suspicious behaviour.
- Use defence-in-depth methods in system design to restrict and control access to individual products and control networks.
- When remote access is required, use secure methods such as Virtual Private Networks (VPNs) with two factor authentication.
- Ensure computer systems are running antivirus software with the latest antivirus signatures.
- If infected, review your antivirus software specific removal guidelines for the malware.
- For other mitigation please refer to the "Strategies to mitigate targeted electronic intrusions" publication. [3]

Links

[1] http://nakedsecurity.sophos.com/2013/10/12/destructive-malware-*CryptoLocker*-on-the-loose

http://blog.emsisoft.com/2013/09/10/*CryptoLocker*-a-new-ransomware-variant

[2] http://technet.microsoft.com/en-us/library/hh831534.aspx

http://support.microsoft.com/kb/310791

[3] https://www.cert.gov.au/advisories

Feedback

CERT Australia (the CERT) welcomes any feedback you may have with regard to this publication and/or the services we provide – info@cert.gov.au or **1300 172 499**.

Note: information sent to the above email address will be in the clear and not secure. Secure communication channels for sensitive information are available on request.

Report an incident

Business partners observing any activity connected to this publication are asked to contact the CERT – info@cert.gov.au or **1300 172 499**.

Reporting cyber incidents allows us to form a more accurate view of cyber security threats and make sure that businesses receive the right help and advice. All information provided to us is held in the strictest confidence. Secure communication channels for sensitive information are available on request.

Business partners who suspect they have been the victim of cyber crime are encouraged to report it to the Australian Federal Police. Cyber crime involves the unauthorised access to or impairment of computer systems and is likely to constitute an offence under the Commonwealth's Criminal Code Act 1995 and/or state and territory criminal laws.

About us

The CERT is the national computer emergency response team. We are the single point of contact for cyber security issues affecting major Australian businesses.

The CERT is part of the Federal Attorney-General's Department, with offices in Canberra and Brisbane. We also work in the Cyber Security Operations Centre, sharing information and working closely with the Australian Security Intelligence Organisation (ASIO), the Australian Federal Police (AFP) and the Australian Signals Directorate (ASD). In addition, we work closely and share information with our international counterparts.

This means we are very well connected and informed, so we are best placed to help businesses protect themselves from cyber attacks.

Traffic Light Protocol (TLP)

TLP classification	Restrictions on access and use
RED	**Highly restricted** **Access to and use by your CERT Australia security contact officer only** You must ensure that your CERT Australia security contact officer does not disseminate or discuss the information with any other person, and you shall ensure that you have appropriate systems in place to ensure that the information cannot be accessed or used by any person other than your CERT Australia security contact officer.
AMBER	**Restricted internal access and use only** Subject to the below, you shall only make AMBER publications available to your employees on a 'need to know basis' strictly for your internal purposes only to assist in the protection of your ICT systems. In some instances you may be provided with AMBER publications which are marked to allow you to also disclose them to your contractors or agents on a 'need to know basis' – strictly for your internal purposes only to assist in the protection of your ICT systems.
GREEN	**Restricted to closed groups and subject to confidentiality** You may share GREEN publications with external organisations, information exchanges, or individuals in the network security, information assurance or critical network infrastructure community that agree to maintain the confidentiality of the information in the publication. You may not publish or post on the web or otherwise release it in circumstances where confidentiality may not be maintained.
WHITE	**Not restricted** WHITE publications are not confidential. They contain information that is for public, unrestricted dissemination, publication, web-posting or broadcast. You may publish the information, subject to copyright and any restrictions or rights noted in the information.
NOT CLASSIFIED	Any information received from CERT Australia that is not classified in accordance with the TLP must be treated as AMBER classified information, unless otherwise agreed in writing by the Attorney-General's Department.