Update from Intersect Systems

Software Systems for Records Management

Arlington, Texas | Fall 2015

Ransomware: Malware for Profit

Recently, Evan Meade of the Fort Worth-based Strickland Group (www.stricklandnetworks.com) made a presentation to the Fort Worth ARMA meeting about the growing problem with ransomware – malicious software that encrypts files on an organization's server, which blocks access to the data, and then demands payment for the decryption key. A ransomware virus typically infects a computer through e-mail or a web site, and then quickly spreads through the computer's access to a connected server, encrypting databases and other files on the server, and then leaving a "calling card" concerning the encrypted files, demanding payment for the decryption key through bitcoin. The first indication a user may have of a ransomware virus infection is a message, when starting a particular database application, that "the ___ database can not be opened due to an unrecognized format."

More recently, in a new variation, some ransomware demands have included a threat to make public information that may be sensitive in nature if the payment is not made.

On five different occasions during the past twelve months, Intersect Systems (www.intersectsystems.com) has assisted several of our customers by identifying sudden problems with database access as a result of ransomware, and by helping identify pre-infection backups to restore. While Intersect's expertise is not normally in addressing malware and related problems, we have helped our customers identify data access problems related to ransomware infections and identify and recover safe backups.

A ransomware infection can quickly become a crisis when an organization suddenly finds that a rapidly growing list of mission-critical databases on a server are no longer accessible.

Recently, Intersect had an opportunity to interview Evan Meade about ransomware, to learn about some of his recent experiences with this growing problem. Evan shared his extensive knowledge as well as some up-to-date information on the problem, and provided several recommendations and precautions that all organizations should be aware of. The interview follows:

Intersect: Evan, there seem to be several different versions of ransomware such as Cryptolocker, Cryptowall, CoinVault, as well as several newer versions of these such as Cryptowall 2 and other variations. What is different in the various versions of Cryptowall, or Cryptolocker? Are the newer versions of Cryptowall, for instance, intended to escape detection that may have been developed and is effective for earlier versions?

Evan: There are differences between the versions, mostly to make the newer versions of viruses more resilient and harder to prevent. One of the main differences introduced in Cryptowall 2 was that the virus-infected PC would then "phone home" by connecting back to the virus author's server connection for an encryption key for the infected file using a TOR connection, which makes tracking where the servers are located nearly impossible. TOR is software available for free which enables anonymous communication, concealing a user's location and making it difficult for Internet activity to be traced back to the user.

In the latest version of CryptoWall, security experts picked apart the virus code and found logic that determines the location of the infected PC. If the infected PC is located in Belarus, Ukraine, Russia, or Kazakhstan, the virus is to uninstall itself from the PC and move on. My speculation is that either the authors are from that region, or the authors are afraid of what those governments would do to them if they are caught. (http://blog.fortinet.com/post/cryptowall-another-ransomware-menace)

Intersect: How do viruses get their names? There seems to be name confusion among some security firms, with some apparently identifying the same virus by different names.

Evan: The viruses have different names at different security providers. McAfee® may refer to a threat by a different name than Symantec,® for instance. In most cases, the names do not come from the authors but from the security experts who analyze and detect the threats.

Intersect: Have any developers or perpetrators of the new phenomenon of ransomware been caught?

Evan: The Department of Justice and law enforcement were able to locate the servers used by the hackers in the first versions of CryptoLocker and take control of the botnet and servers. They actually took control of the servers and neutralized the threat. Here is a very interesting article about the takedown:
http://www.computerworld.com/article/2489997/security0/feds-declare-big-win-over-cryptolocker-ransomware.html

Intersect: Why hasn't the NSA, with all of the post-Snowden publicity about their technology and spying capabilities, contributed to addressing the ransomware problem? Or has NSA contributed? Symantec identified the very sophisticated Stuxnet virus – an impressive accomplishment – but why not the CIA or NSA? This is a question we get asked.

Evan: I think the security industry is behind on the threats that are out there. We are seeing news reports more and more frequently about high-profile hacks and incursions into secure networks. I also think it's just going to get worse because there are so many different systems, each with its own vulnerabilities and weaknesses. Two that stand out are the Target hack in 2013 where 40 million credit cards were stolen and Target ended up paying $67 million dollars to settle. See the following hyperlink: http://money.cnn.com/2013/12/18/news/companies/target-credit-card The other major incident that really concerns me is the Office of Personnel Management hack in June of 2015. In this incident, extremely sensitive information such as SSNs, fingerprint data, security clearance info, etc. for 22 million current and former government employees was stolen. Security experts believe that the government of China was behind this cyber-attack and can only speculate on why they wanted the data.

Intersect: I note that some of our customers have seriously limited employee access to e-mail and web sites from their computer stations, while many more are unbelievably open. Are there any particularly good resources or security tools that can be helpful with this? Some such as McAfee and Symantec have some protections that flag suspect web sites, but how effective are they? We also find MalwareBytes® and MalwareBytes Anti-Exploit® with some of our users. How much can an organization depend on these or other similar sources of protection against ransomware, as opposed to other viruses and malware?

Evan: We are constantly re-evaluating the security tools that we use and recommend. The rate of new security threats released into the wild on a daily basis is staggering and a layered approach to security utilizing multiple products at each path is very important. Currently, I recommend Malware Bytes as well as OpenDNS Umbrella® which maintains a real-time list of servers that are hosting malicious traffic and can block that traffic before it gets to a network.

Intersect: Can you provide a checklist for our customers that they can share with their employees in order to help protect against ransomware and similar threats?

Evan: Here are some Healthy Computing Tips:

- Keep antivirus software up to date
- Take regular backups, and keep them offsite
- Use an external security device like a packet inspecting firewall
- Block internet traffic that you don't need – for example, TOR, i2p, and other peer to peer protocols.
- Don't click on links in emails and don't open attachments unless you know the sender or are certain they are valid.
- Keep ALL your software up to date (Windows, Office, Acrobat, Java, Flash, etc.)

Intersect: How can organizations contact The Strickland Group, and does The Strickland Group have an emergency hot-line for weekend or after-hours contact from an organization that discovers a problem at an inconvenient time?

Evan: Our helpdesk line is 817-224-2100. Customers can leave a message on this line 24/7 and our on-call engineers will be paged with that message.

Intersect: Thanks, Evan, for spending time with us today on this important subject.

About The Strickland Group:

The Strickland Group, Inc. is a team of enterprising consultants whose talents and experience extend across a broad scope of Information Technologies. We provide our services to all spectrums of the business world. Our areas of expertise are:

NETWORK INFRASTRUCTURE – The Strickland Group has expertise in design and implementation of Information Systems architecture including network design, server systems design, virtualization architecture, operating system configuration, router / switch / firewall programming, server monitoring and management and help desk solutions. Our Network Operations Center team based in Fort Worth, Texas works with clients small and large for all their Information Technology needs.

CUSTOMIZED INTRANET/EXTRANET DEVELOPMENT – The Strickland Group also has expertise in web/database applications. TSG can design customized web-based business tools tailored to help your company accomplish its business objective and corporate goals.

Windows and Office are trademarks. or registered trademarks. of Microsoft Corp. Acrobat and Flash are trademarks of Adobe Systems Inc. JAVA is a trademark of Oracle Inc.

*Intersect's **Update** newsletter is published periodically for users of Intersect records management systems with news, announcements, and update notices as appropriate.*

***The Intersection** is published periodically with more comprehensive articles on topics related to records and document management, as well as features of general interest on selected users of Intersect's records management systems.*

Contact Intersect by e-mail at intersect@newintel.com Tel. (972) 641-7747 Visit our web site at www.intersectsystems.com

Copyright © 2015 by Intersect Systems Inc.