C5C Monthly Cyber Newsletter
Category 5 Consulting, LLC
38 Washington Square | Newport, RI
www.Category5llc.com
401.451.8037

Ransomware

How to Avoid Becoming a Victim

Ransomware is a form of malicious code typically employed by cyber criminals to hold your company's data hostage. This is accomplished when the malicious code exploits a pre-existing vulnerability on one of your company's computers and then encrypts specific files on the hard drive. Depending on the strain of ransomware, a victim can usually expect to have most of their Microsoft Office documents (.docx, .xlsx, .ppt), Adobe Acrobat documents (.pdf), and photos (.jpg, .gif, .png) locked and no longer accessible. The victim will then see a message pop up on their screen instructing the victim how to pay a ransom, usually in the form of crypto currency (an anonymous online currency) such as Bitcoin, to decrypt their data. Until you pay the ransom, you will not have access to your critical data!

Victims are usually targeted with ransomware in two ways. The first way is via a socially engineered email where a victim will receive an email with some type of "Purchase Order" or "Contract" theme. The victim will open the email and then open the malicious attachment or click on the malicious link in the email body. The second way is via a website "drive-by" which occurs when a threat actor compromises a

There are a few simple steps that you can implement right now to avoid becoming the next victim of ransomware.

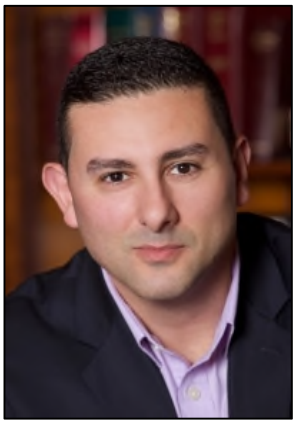
Quick Tips to Avoid a Compromise

- Make sure that all systems are routinely patched to include operating systems, software updates, and anti-virus definitions. This includes Microsoft Office, Adobe Acrobat, and any internet browser you typically use
- Schedule frequent backups of all important servers and workstations and ensure that some backups remain air-gapped (unplugged from any machine)
- Educate your staff on how ransomware propagates and to not open any suspicious attachments or click on any suspicious links in emails, especially if it is from an unknown sender
- If a ransomware compromise is suspected, immediately disconnect the machine from your network but keep it powered on. This allows an incident responder to perform critical forensic memory analysis that is otherwise lost when you power down your machine.

legitimate website and then hosts malicious code on it. Essentially, anyone who visits the compromised site with a vulnerable machine will download and execute the malicious code. There is no way to actively avoid these kinds of attacks.

It is prudent to back up your entire system. In the event of a ransomware event, you can quickly access your data and restore your website. The only defense against such tactics is to ensure that your internet browser is up to date and your anti-virus software has the latest update and is fully protecting your machine.

Contributors:



Brandon Catalan, CCE, CISSP is a Managing Partner of Category 5 Consulting, LLC. His background includes conducting thousands of classified and unclassified cyber espionage intelligence operations, computer forensic examinations, and advanced incident response actions in support of the US Intelligence Community and the Defense Industrial Base. He is also a Lecturer at Salve Regina University where he teaches Advanced Digital Forensics, Malware Forensics, and Cyber Intelligence. He holds graduate level degrees in National Security and Digital Forensics and is also a member of the International Society of Forensic Computer Examiners which certified him as a Certified Computer Examiner (CCE).

Stephen Ucci, Esq. represents domestic and international clients in a variety of transactional matters for the Law Offices of Adler, Pollock & Sheehan. He advises clients in the United States and abroad on government contracting, anti-corruption compliance, organizational conflicts of interest, government security clearance matters, business formation, joint ventures, teaming, financing, cyber security, privacy matters, mergers, acquisitions and divestitures. His clients range from Fortune 500 companies to start ups. Stephen regularly lectures on cyber security, privacy, big data, drones, trade secret protection and regulatory compliance. He is serving his seventh term as a member of the Rhode Island House of Representatives.