Secure Ideas professionally evil℠

Customer Intelligence Bulletin

May 17, 2017

Media reporting on the WannaCry ransomware campaign has contained exaggeration, bad information, and fear tactics. This Bulletin seeks to provide Secure Ideas customers situational awareness about malware, ransomware, and phishing campaigns in the wild, and to provide a basic plan for businesses.

The Secure Ideas Perspective

Coverage of the WannaCry ransomware campaign has been dramatic, and caused tremendous concern among businesses. Don't be distracted by media reports, which have been off-mark since the beginning: WannaCry is not unprecedented, it is not unique, and it doesn't matter if it comes from North Korea or North Carolina. It is much more important to understand that ransomware is especially damaging to those without backups, so patching systems and backing up data off-site are very important. Patching and updating of all systems must be regularly conducted, and most important, full backups – and *not just* file-based backups like Dropbox – must be maintained.

What is Ransomware? What Is Malware?

Malicious code, or **malware**, is a generic term used to describe viruses, worms, ransomware and basically anything that runs on a computer with malicious intent, outside of the user's desires. Historically, malware might be code that runs in the background, unnoticed or simply cause a machine's sluggish response that a user may or may not notice.

As with weeds, malware is in the eye of the beholder – just as a rosebush is a weed in a wheat-field, certain tools like keyloggers and toolbars can be used for good, as well as evil. Some malicious code might gather information about a user so that companies may better target ads; other code might be to speed up a centrifuge or an electrical generator to cause physical damage.

Ransomware is a form of malware that stands out for its destructive capabilities, and because its prey is, unfortunately, the most vulnerable users and companies: those who have not spent the time and effort to provide security and make backups of their data.

The groups most vulnerable to irreversible data-destruction by ransomware those who:

- Do not (for whatever reason) regularly patch, or update, their operating systems and applications;

- Do not have backups of their data; and
- Do not have a robust, and tested, plan for disaster recovery and incident response in place.

Ransomware Is Harder Than Other Infections to Remove

Without reversing the cryptographic code that encrypted the data, it's difficult (but not impossible) to find the key. But it takes a long time – measured in days and weeks, not minutes and hours. Meanwhile, your business is down, which costs you money. Without pre-arranged, tested, and solid procedures of data recovery, companies must either rebuild, or pay the ransom and hope that the decryption keys are provided by the criminals. Unfortunately, there's no promise to be made that your data will be restored to you after you pay or that you won't get hit again by something similar. In the case of WannaCry, there have been more than a thousand companies that have paid ransom, and to date, no recoveries have been made.

Backups versus Snapshots

Many larger corporations make regular backups, but many smaller firms back up just the data – using a service like Dropbox – and not the entire computer. File backup services like Dropbox are not a disaster recovery solution, they are intended to be a data recovery solution. This means that in a situation like ransomware, in which the entire system (operating system, applications, as well as data) must be replaced, it takes significantly longer to recover. With a snapshot, the image of yesterday's (or this morning's) computer can be restored, the machine restarted, and we're back to business. With incremental data restoration (such as Dropbox), information technology staff must wipe the hard drive, reinstall Windows, reinstall the applications, and then download and restore the lost data. This takes hours per machine to accomplish.

Testing Backups

Businesses have only recently begun to focus on testing the backups they've made. Sometimes, the restoration process doesn't work, and a misconfiguration can be detected. It's important to have a proper procedure that will withstand an emergency and function as expected.

Physical Disaster Recovery

Similarly, many corporations also don't have a disaster recovery site that they can use in the case of a physical disaster such as a hurricane, tidal wave, major storm, plane crash, or incident of terrorism or civil unrest. Companies without pre-arranged infrastructure and solid procedures of both cyber (data) and physical recovery are forced to "start over" in the event of a crippling disaster. Ransomware would be just one example of this.

What Ransomware Tells Criminals About Your Organizational Maturity

When an organization is hit by ransomware, and they are unable to immediately recover, criminals understand that this organization has not invested in some fundamental technologies, procedures, and practices. Those organizations without tested snapshot backups and restoration capabilities have also likely not invested in redundant systems to protect employee data, financial data, and business-critical data and processes. This is not a declarative conclusion, but it is a safe assumption, and criminals prey on the weak. This paints a target on your company, and you can expect follow-on attacks.

Why Paying Ransom is a Terrible Idea

If it is revealed publicly that you paid the ransom, criminals assume it's likely that any other denial of service attack might be worth their investment – you are a payer.

The Basics

Every dollar spent proactively is worth $100 to fix problems; every minute of prevention is worth hours of incident response. Another valuable benefit of having these basics in place is that doing so, and documenting it, can reduce – sometimes significantly – risk and cyber insurance premiums.

Secure Ideas believes that a robust program of security isn't something you can buy, it's something that must be built, and culturally assimilated. SI can help you understand the basics, and help with a range of programs including security assessments, architecture reviews, and programs of training and testing appropriate to your firm's unique situation.

At a minimum, we believe companies must consider the following:

Disaster Recovery Plan

The first thing we suggest is having a disaster recovery plan. This can be accomplished in a relatively short time-span, and a significant side-benefit of the exercise is a dramatically increased situational awareness of the processes, procedures, systems, and people most important to your business. A DR Plan is created by identifying, prioritizing, and documenting which assets are critical to your company's revenue-producing activities - including those assets on which more critical assets are dependent. DR is the process of creating redundancy – a second set of everything you need, stored somewhere else, synchronized, and ready to go at a moment's notice.

The regular testing of disaster recovery capabilities is essential.

Configuration Management, Patching, & Updating Program

All software has bugs; all software has security vulnerabilities. And software is constantly evolving. This is why updating, upgrading, and making emergency repairs (a "patch") is so critical. To truly reduce risk, businesses cannot treat patching as an exceptional event. Instead, patching, updating, and managing configuration of all computers must be considered an ongoing maintenance program. Owners of processes, business units, change management, procurement, and IT must all be committed to this process for the program to be successful. It's not a panacea – some vulnerabilities exist for which patches have not yet been developed. But you substantially reduce your attack surface and likelihood of being exploited through a comprehensive configuration and patch management regime.

Incident Response Plan

The Secure Ideas Response Team likes to say that the worst time to think about an incident response plan is during an incident. Your company should have at the very least a process through which you can understand an event, and evaluate it to determine if it meets the criteria under which you can declare a cyber security emergency and begin to recover. The Secure Ideas Response Team can help you develop and maintain such a plan, and retainers are available to ensure your time to insight and repair is minimized.

##

About Secure Ideas

Secure Ideas is an independent security-consulting and penetration testing firm focused on providing organizations with the services and knowledge needed to improve the security posture of their computing and network environment. Our services are designed to not just identify vulnerabilities, but to provide actionable recommendations and to promote a Security State of Mind.

The core of our service offerings is comprised of a talented team of Security Consultants and Penetration Testers who have experience with security assessments for networks, web applications, mobile apps, social engineering, physical security, embedded, wireless and more.

To augment penetration testing, Secure Ideas offers Scout: a service designed for frequent testing at a competitive price point. Scout can accommodate several types of tests, including network, web applications, PCI, and users.

Secure Ideas believes we need more good-guy hackers out there if we are to keep up with the bad guys, so we do what we can to share our knowledge. This includes webcasts, recorded content, and full-fledged hands-on training. More information is available at https://secureideas.com

About the Secure Ideas Response Team

When your company is experiencing a computer breach or emergency, the Secure Ideas Response Team (SIRT) can help. Created and staffed by professionals with decades of experience through hundreds computer emergencies, security assessments, root cause analysis, network forensics, re-architecture, and design, SIRT will begin the process of helping you within an hour of your call.

Our broad base of experience includes cyber incidents at financial services, manufacturing, medical, chemical, and oil and gas firms. We specialize in response to malware, ransomware, botnet and remote-access Trojan attacks. We have worked extensively on cases of intellectual property theft by criminal gangs and nation-state actors. Our principals have successfully liaised with state and federal law enforcement, and have unique and significant experience in that arena. We have successfully worked with the smallest, and the largest, organizations in the country.

Our services include immediate and short-term recovery re-architecture, and we work with you once we have stabilized your environment to ensure the breach does not re-occur so business can carry on.

About This Report

This report was written by Kate Vajda (Secure Ideas), Nick Selby (Secure Ideas Response Team) and Moeed Siddiqui (Secure Ideas Response Team).