Ransomware

Ransomware is getting worse.

What is Ransomware?

Ransomware is a form of malware which has been around almost as long as personal computers have existed. This form of malware is called ransomware because it restricts access to the infected computer system or data in some way, and demands that the user pay a ransom to the malware operators to remove the restriction and/or get access to your files again.

Ransomware is introduced into the computer environment most commonly through email with a malicious file attachment or link, but it can also be acquired through visiting infected websites and other methods.

Some forms of ransomware are known as crypto-ransomware. In the news they frequently refer to Crypto Locker which is a very prevalent form. This type systematically encrypts most of the files on the system, which prevents them from being opened, while some may simply lock the system rendering the system unusable.

Proxios' current Best in Class technologies, people and processes are designed to fight malware.

What do we do now?

Proxios employs a robust, in-depth defense process to handle ransomware. But as malware continues to increase in sophistication, which it ALWAYS will, we will have to employ newer technologies designed to fight this ever-increasing threat.

Our current process is a combination of:

(1) Employing a dedicated Information Security Officer.
(2) Utilizing the following prevention methods to stop the malware from reaching the user:
    - State of the art advanced Firewalls at all entry/exit points.
    - Best in class Anti-virus / Anti-malware software, updated regularly.
    - Spam and spoofing filtration on all inbound and outbound email traffic.
    - Installation of the most recent software security patches.
(3) Using detection methods to quickly identify any malware that is activated.
(4) Apply a complete Incident Response for Containment and Resolution
(5) Deploy recovery methods to quickly restore the users back to a clean state.

The above technologies and processes cannot and will not be able to catch all instances of malware; therefore, there is a strong need for the end user to be prepared to avoid introducing the malware to the environment.

We are looking at adding even more capabilities to enhance protection of our clients.

What are we doing?

Proxios is currently looking at adding additional, advanced technologies that are specifically suited for these newest and quickly evolving forms of malware, focusing on how they are introduced into our clients systems.

Our plan is to use a combination of:

(1) Implementing new features and functionality for our existing technologies:
- Enhancing our existing systems to ensure that the latest capabilities are available where needed

(2) Utilizing products that provide Targeted Threat Protection:
- Protection against Spear Phishing attacks (Impersonation Protect).
- 67% Increase in this type of attack during 1st quarter 2016 alone.
- URLs re-written in incoming emails.
- Administrator Notifications.
- Threat Dashboard and Granular Logging.

(3) Provide Next Gen services that achieve new Advanced Threat Protection:
- Next Gen IDS/IPS
- Next Gen SIEM
- Advanced Forensic Hunting and Remediation
- Complete Incident Response for Containment and Resolution
- Attack Pattern and Behavior Based

(4) Deliver Managed Security Awareness Training:
a. Formal programs to provide on-going awareness and training for users

Users are a VITAL part of malware defense.

Users are one of the most vital components to defense in the on-going and continually evolving cyberattacks threat scenario. Below are examples of the most common ways these occur, and what users must think about and remember:

Hackers know that most people tend to be helpful and trusting, so they execute attack strategies that exploit human vulnerabilities:

- **Email** – Malware often arrives on your PC in an email attachment. You should never open an email that looks suspicious or an attachment from someone you don't know. Pay attention to the sender's email address as well as who it's addressed to, as that may provide a clue that something's not right. Instant messages and requests for file transfers can also spread malware.

- **Websites** – Never open links to webpages that you don't recognize or that are sent from people you don't know. Look closely at the spelling of the website name. At first glance, it may look familiar, but upon closer examination you may find it is spelled slightly wrong. Malicious websites can install malware on your PC when you visit them.
- **Use caution on the Virtual Desktop** – If you view a website that doesn't look quite right, or unexpected things happen when you visit, immediately call the Proxios Help Desk.
  Use caution on your local PC – If you view a website that doesn't look quite right, or unexpected things happen when you visit, close your browser; download the latest updates for your security software; and run a quick scan on your PC. Call the Help Desk of whoever supports your local PC.
- **Pirated software on your local PC Only** – Malware is often bundled together with pirated software. When you install the pirated software, you may also install malware. If you think that any software that you have on your local PC is pirated, check with the software vendor, and they can help you confirm if the software is safe or not.
- **Social engineering** – Malware authors often try and trick you into doing what they want. This can be clicking or opening a file because it looks legitimate; paying money to unlock your PC; or visiting a malicious webpage. These deceptive appeals are known as social engineering. Never click a link in an email that says you need to log in because your account has been locked, or indicates some problem with your account. If you think it might actually be something you need to do, **do not click any link in the email**. Instead, in a browser window, go to the website yourself and log in. It will then tell you if you actually need to do something. If it's a company that you don't even know or deal with, it definitely should just be deleted.
- **Passwords** – Attackers may try to guess your Windows or Apple account or other passwords. This is why you should always use a password that can't be guessed easily. A strong password has at least eight characters (longer is better) and includes letters, numbers, and symbols.
- **USB flash drives and other removable drives** – Some types of malware, such as worms, can spread by copying themselves to any USB flash drives or other removable drives that are connected to your computer. Always be careful when sharing removable drives, and make sure you scan them with anti-virus and anti-malware scanners before you do anything else with them.

Proxios continually evaluates the latest safety risks to ensure our clients are always protected.

As you can see from all of the above, which only lightly touches on the level and complexity of today's cyberattack threats, this is a never ending challenge requiring the

on-going attention and commitment of everybody to stay ahead. As we make available many of the new capabilities mentioned above, there will likely be costs associated with each. Luckily these costs can be spread across our large client base, since most individual companies do not have the resources (large budget needed, highly trained specialized staff, time etc.) to accomplish the above on their own.

Proxios will continue to evaluate, plan and take appropriate actions to ensure that we, and you, are protected as much as possible. We will be continuing to communicate our progress as we enhance our services and offerings to address this on-going need. If you have any questions about anything contained in this communication, please feel free to reach out to your Service Delivery Manager.