ePlus Solution Brief

Stop Disruptive Cyber Threats

Mitigate the risk disruptive cyber threats, such as ransomware, pose to critical business operations.

Ransomware and other malicious software can have a devastating effect on business operations and brand reputation. The best way to protect your organization is with a comprehensive security program that spans your entire IT infrastructure. ePlus provides technology and services to help our clients mitigate the risks associated with ransomware and other disruptive malware for proper threat prevention and detection.

What are Disruptive Threats?

Malicious software that is created and deployed with the intent of damaging and disrupting critical business functions. The most frequent example, ransomware is used by cyber criminals to lock and hold files and/or access to computer resources for a monetary ransom. Additional forms of disruptive malware include cryptojacking or using an unauthorized computer to mine cryptocurrency, and any unauthorized software that enables unauthorized control, degradation, or loss of service to a system or computing resource. Disruptive malware can have a long and lasting effect on business operations.

Who is at Risk?

Everyone. Recent data breaches by way of ransomware and other malicious software have been seen in industries from retail to healthcare, even impacting educational institutions and state and local governments.

By 2019, ransomware damage costs are expected to hit **$11.5 BILLION**.

Damage from the Atlanta ransomware attack has crossed **$10 MILLION** and continues to climb.

What Impact Could a Malicious Cyber Attack Have?

Malware and its ability to disrupt business operations have a far reaching effect on the goods and services organizations provide across many industries. A few examples:

- The loss of business continuity can put critical services in jeopardy.
- Healthcare organizations have substantial impact to life and safety if necessary systems are not online.
- Municipalities may suffer from inability to provide critical services and put community safety at risk.
- Utilities may suffer inability to deliver power, water or other highly dependent resources.
- All organizations risk a significant impact on brand reputation.

How ePlus Can Help

ePlus provides technology and services to help our clients mitigate the risks associated with disruptive malware for proper threat prevention and detection. We help navigate the sea of solutions and software to provide you an efficient, integrated and affordable solution. We work with your organization and understand the skills, processes and technology you have made investments in and will tailor our approach to ensure your organization is best positioned to mitigate this critical risk.

CONTACT US

Contact us today to learn more about how the ePlus approach to Stopping Disruptive Threats can be tailored for your environment.

eplus-security@eplus.com
1-888-482-1122
www.eplus.com/security

Where Technology Means More®

THE EPLUS APPROACH TO STOPPING DISRUPTIVE CYBER THREATS

ePlus leverages partnerships with leading technology providers and couples that with deep technical knowledge and experience to provide a comprehensive approach to threat prevention and detection. As a risk or an attack can present itself at any stage in the cyber-attack lifecycle, ePlus addresses each phase head-on.

PREVENTING MALWARE DELIVERY

Malware is most often delivered to host systems via web and email. Leveraging threat intelligence to help identify malicious websites via DNS lookups provides a basic security hygiene approach to ensuring your web traffic is not unknowingly directed to sites that could contain malware.

Email security technology will also provide protection against receiving email from malicious domains and with weaponized attachments.

DETECTING MALWARE BEHAVIOR

The endpoint or host can provide the next level of protection against installation of disruptive malware by employing an endpoint agent that is capable of detecting when malware installation has been invoked and will identify the behavior, stop the installation, and report the necessary activities to the IT security team for further processing and recovery actions.

Advanced endpoint security solutions provide the most capable and robust methods of identification and eradication of malware and suspicious behaviors.

END USER AWARENESS

If the controls you had in place were not able to prevent the malicious payload from reaching the end system, it is important to have the user/operator of that system trained to help identify suspicious websites, email and attachments and subsequently educated to not open, click, or install anything that may be suspicious.

User awareness education is an important step for IT and non-IT positions in an organization as it helps to promote a heightened awareness around the risks associated with cyber threats. User awareness training is often delivered on a regular basis through online training modules with skills assessments.

EMPOWERING RECOVERY

The biggest challenge in cyber security today is that no solution is 100% effective at preventing cyber-attacks. The recommended methodology is to use the processes and controls available to mitigate risk in accordance with your organization's risk profile.

In the event critical data sets or systems have been encrypted and rendered unusable by malicious software, it is important to invoke a response process that will help identify and contain the malware outbreak and restore normal business operations.

This typically includes the use of **incident response services** and the use of near **real-time backups**.

Cyber Security Frameworks

ePlus provides advisory services to help companies pursue alignment to leading industry frameworks such as CIS and NIST.

Indicates control is either fully or partially addressed by this ePlus solution.

CIS CONTROLS ADDRESSED

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

NIST CYBERSECURITY FRAMEWORK ALIGNMENT

IDENTIFY

ID.AM	ID.BE	ID.GV	ID.RA	ID.RM	ID.SC

PROTECT

PR.AC	PR.AT	PR.DS	PR.IP	PR.MA	PR.PT

DETECT

DE.AE	DE.CM	DE.DP

RESPOND

RS.RP	RS.CO	RS.AN	RS.MI	RS.IM

RECOVER

RC.RP	RC.IM	RC.CO

Corporate Headquarters:
13595 Dulles Technology Drive
Herndon, VA 20171-3413

Nasdaq: PLUS