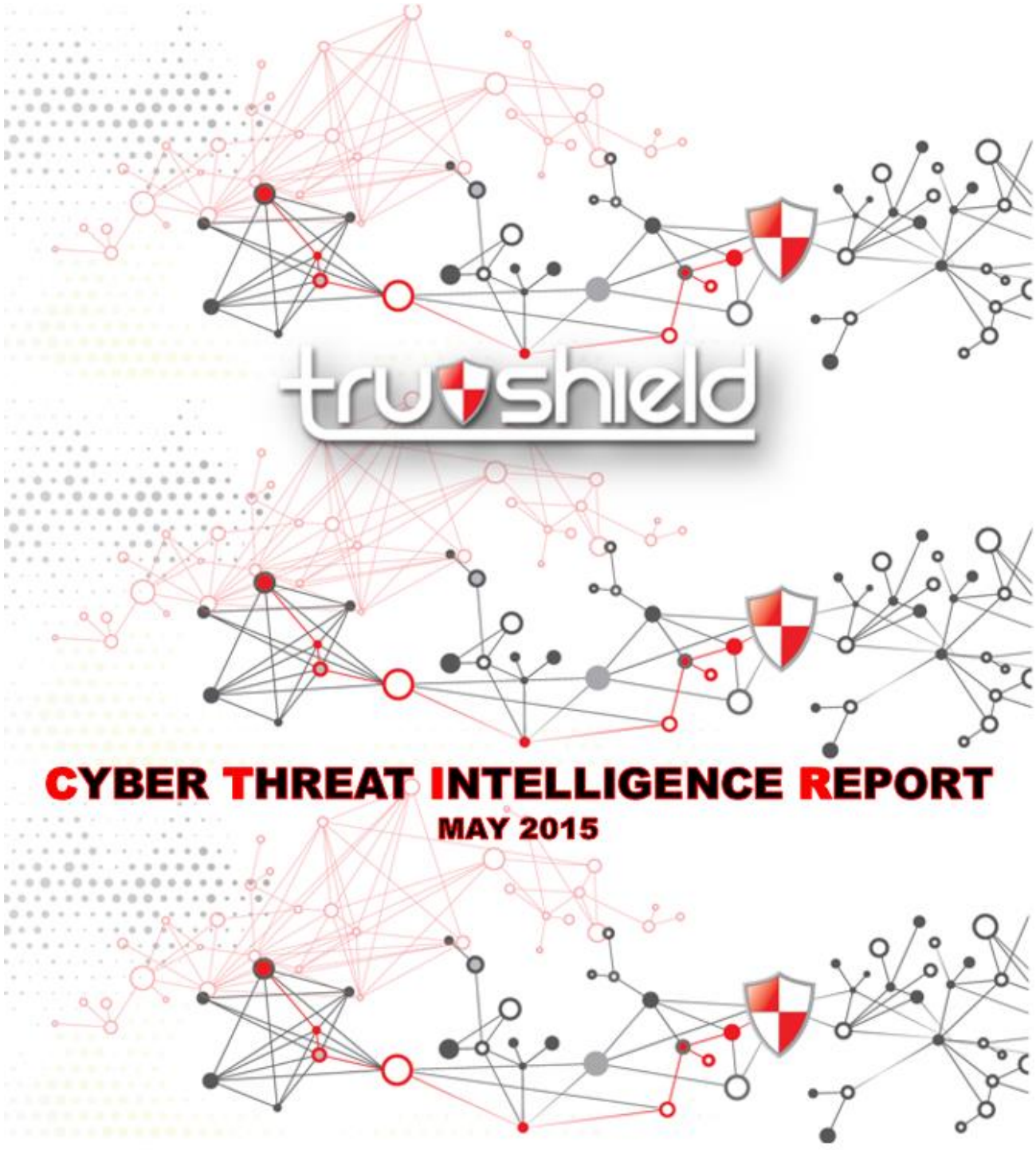


CYBER THREAT INTELLIGENCE REPORT

MAY 2015

CYBER THREAT INTELLIGENCE REPORT – MAY, 2015

DETECT. DEFEND. RESPOND. NEUTRALIZE.

TruShield Security Solutions is a global cyber-security company operating on several continents across multiple industries. Our core clients spans from government, critical infrastructure, not-profit, legal, retail, and financial industry. We provide Continuous Security Monitoring to our clients in order to ensure compliance with the strictest regulations and enterprise risk management. With a unique combination of people, processes and technology, we've developed a proven method for detecting and preventing attacks against our clients' digital assets and networks.

Our global Security Operations Centers combined with our state-of-the-art global Cyber Threat Intelligence Center (CTIC) aggregates, correlates, analyzes, and investigates more than one billion events per day. We collect data from hundreds of thousands of endpoints including laptops, tablets, and smartphones. We also monitor and manage thousands of security appliances and technologies including:

- Security Information and Events Management
- Next-Generation Firewall
- IPS and IDS
- Unified Threat Management
- Internet and Mail Gateway
- NAC, MDM and DLP
- Identity Access Management
- Network Behavioral Analysis platform

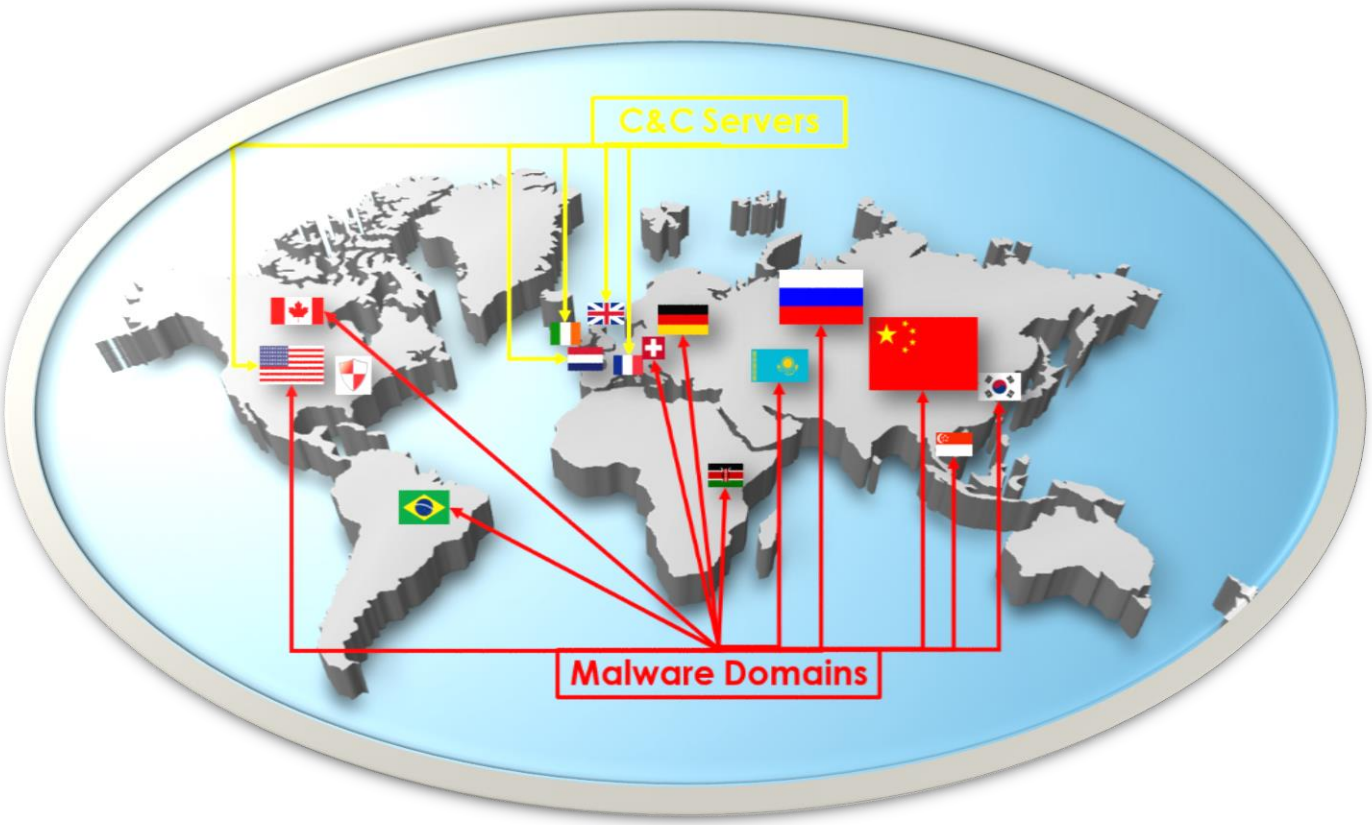
May 2015 General Findings

36 Billion events processed

During the month of Month we have collected and categorized close to 36 billion events. After the full cycle of correlating and aggregating raw data we determined that 475 events posed various degrees of risk to our clients. More importantly we found attack sources generated from IPs located in US, China, Netherlands, Russia, and France. In addition, we noted attempts from Korea, Ireland, and- a novelty for this month- Switzerland and Brazil.

Top 10 C&C Servers and Malware Domains			
Malware Domain	**Country**	**C&C Server**	**Country**
Driveake[.]webcindario[.]com		w9c[.]rzone[.]de	
nonobabe[.]100webspace[.]net		cluster015[.]ovh[.]net	
mymoney[.]000a[.]de		cambridge[.]noc40[.]com	
legendastar[.]ru		lb1[.]namesco[.]net	
ngusto-uro[.]ru		vtunnel[.]org	

Table 1: Internet Threats



Picture 1: Geolocation of Cyber Threats

In May we detected, blocked, and neutralized more than 1,200 attacks against our clients' networks. Our security analysts relentlessly worked to mitigate risks to confidentiality, integrity, and availability of data in the critical infrastructure and other industries. Behind the majority of these attacks we identified government and state-sponsored cyber-attacks, cybercrime rings, and commercial cyber espionage. The leading countries that host the most malicious IPs were China, The Russian Federation, United States, Netherlands, and France. Also a smaller number of malicious IPs and malware domains were based in Kazakhstan, Spain, Germany, and Kenya.

Another major attack vector was represented by malware delivered via multiple vectors, including email, drive-by downloads, mobile devices, and USB devices. For instance, our CTIC was able to determine that close to 50 different malware families were targeting multiple industries during this period.

MALWARE TYPES DETECTED ON ALL INDUSTRIES		
C&C AND Backdoor Malware	**Worms, Downloaders, Exploit kits**	**LINUX, Banking malware, Ransomware**
Win.Trojan.Backspace Win.Trojan.Bancos Win.Trojan.Banload Win.Trojan.Bartallex Win.Trojan.Beebone Win.Trojan.Bedepshel	EXPLOIT-KIT Sweet Orange EXPLOIT-KIT Angler	Win.Trojan.TeslaCrypt

Win.Trojan.Cheprobnk Win.Trojan.Dalexis Win.Trojan.DesertFalcon Win.Trojan.Fareit Win.Trojan.Farfli Win.Trojan.Fulairo	EXPLOIT-KIT Fiesta	Win.Trojan.CryptoWALL
Win.Trojan.Kraken Win.Trojan.Kriptovor Win.Trojan.Mantal Win.Trojan.Mathanuc Win.Trojan.Mudrop Win.Trojan.Nalodew	EXPLOIT-KIT Styx	Html.Phishing.Crea
Win.Trojan.Odlanor Win.Trojan.Pvzin Win.Trojan.Simda Win.Trojan.Tendrit Win.Trojan.Sanhotan Win.Trojan.Zinnemls	Win.Worm.Klogwjds Win.Worm.Mozibe	MacOS.Trojan.MacVX
Backdoor.Win32.Chkngrbot.A Win.Backdoor.Cybergate Win.Backdoor.Nirunte Win.Backdoor.Plez Win.Backdoor.Wekby Torn	Linux.Downloader.Mumblehard Win.Downloader.Siromost	Linux.Trojan.Mumblehard

Table 2: Most representative malware signatures collected in May

Attack Vectors Analysis

Top 5 most critical attack vectors

As seen in the previous table, we have experienced Windows, MAC, and Linux specific malware. In addition we identified malware responsible for backdoor communication with botnets and C&C servers, ransomware, Trojans, worms, exploit kits, and spamming malware. In addition to malware-based attacks we've experienced multiple attempts to exploit recently discovered application vulnerabilities such as Venom and Magento.

- **LINUX Mumblehard** – First reported by security experts from ESET, this family of malware targets web servers running both the Linux and BSD operating systems. A Mumblehard infected server opens a backdoor for the cybercriminals that allows them full control of the system by running arbitrary code. It also has a general purpose-proxy and a module for sending spam messages. The founder of the Mumblehard exploit identified 8,867 unique IP addresses and linked the attacks to YELLSOFT (yellsoft[.]net) which is a company that sells DirectMailer software for delivering bulk mail and is believed to be based in Russia.

  According to ESET "Mumblehard components are mainly Perl scripts encrypted and packed inside ELF binaries. In some cases, the Perl script contains another ELF executable with the same packer in the fashion of a Russian nesting doll". Our security analysts identified and blocked two instances of Mumblehard which both had two individual components. The first

part was a downloader that has the role to deploy additional malware. The second component was the actual Trojan responsible for C&C backdoor communication and SPAM distribution.

- **SIMDA Botnet (US-CERT Alert TA15-105A)** – Our Security Operations centers experienced multiple malware-based attacks using Simda Trojan. More than 770,000 computers were detected worldwide as being members of the Simda botnet. Interpol Digital Crime Centre (IDCC) worked with Microsoft, Kaspersky Lab, Trend Micro and Japan's Cyber Defense Institute to dismantle this botnet. Our SOCs successfully detected and blocked all Simda malware delivery attempts.

- **VENOM Vulnerability (CVE-2015-3456)** – Our defense-in-depth technologies detected attempts to exploit this vulnerability. Venom is a buffer overflow vulnerability in QEMU's virtual Floppy Disk Controller (FDC). The vulnerable FDC code is included in various virtualization platforms and is used in some Oracle products. The vulnerability may be exploitable by an attacker who has access to an account on the guest operating system with privilege to access the FDC. The attacker may be able to send malicious code to the FDC that is executed in the context of the hypervisor process on the host operating system. It is important to highlight that the attacker cannot remotely exploit Venom, instead it has to have authentication credentials which can still be retrieved via other exploits. Oracle urges applying security patches.

- **MAGENTO Vulnerability (CVE-2015-1397, CVE-2015-1398, CVE-2015-1399)** – Magento vulnerability was recently discovered by our colleagues at Checkpoint. The Remote Code Execution allows attackers to completely compromise an e-commerce platform provided by Magento (subsidiary of eBay). The vulnerability is actually comprised of a chain of several vulnerabilities that ultimately allow an unauthenticated attacker to execute PHP code on the web server.

  The vulnerability does not reside in any of the plugins available, instead it exploits Magento's core. The attacker bypasses all security mechanisms and gains control of the store and its complete database, allowing credit card theft or any other administrative access into the system. It is critical to apply patches released by the vendor in order to protect the confidentiality of sensitive data hosted by web stores running on this platform. Our clients in the financial and retail industries were safe against this vulnerability due to our advanced IPS and alerting capabilities.

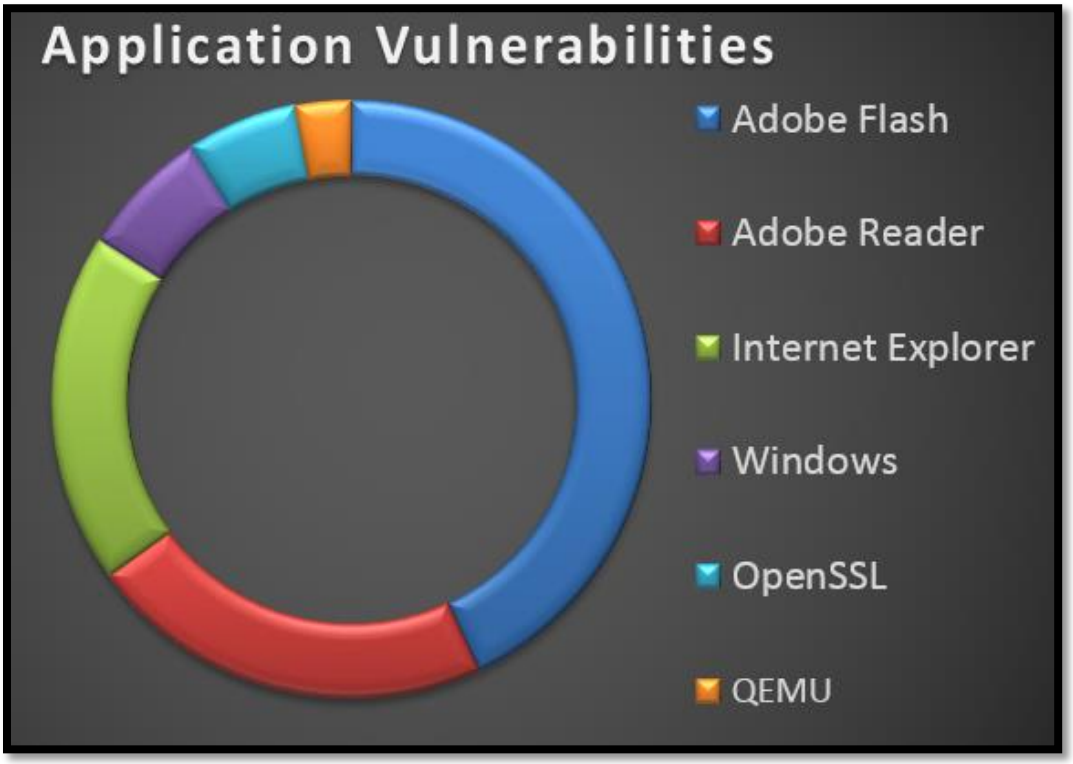
- **RANSOMWARE TeslaCrypt** – Ransomware has been on the rise for the last 3 years. TeslaCrypt is one of the newest reiterations of this type of malware that denies a user access to their own computer. Ransomware usually requires small amounts of money in the $200-$300 range, only allowing access to resources after the victim pays the ransom. This malware usually targets Microsoft-based systems and encrypts the content of the hard disk, rendering it impossible for the victim to gain access.

Ransomware no longer impacts individual users and home computers. According to the FBI, organizations from all industries can become infected with it, resulting in the loss of sensitive or proprietary information, a disruption to regular operations, financial losses incurred to restore systems and files, and/or potential harm to an organization's reputation. What is interesting to note is that our multiple defense technologies detected the Exploit Kit Sweet Orange to be responsible for delivering TeslaCrypt ransomware, which was validated by third-party findings.

Operating systems and application attacks

33 % increase in application exploits

During the month of May we continued to experience an increased number of attacks based on applications' weaknesses. Among the most important applications targeted by attacks were Microsoft, Adobe, Novell and Oracle. The biggest player was Adobe which continues to show multiple vulnerabilities, which are abused by the Exploit Kit Fiesta. Also, Fiesta is responsible for crashes and other misuses in Java and Microsoft Silverlight.

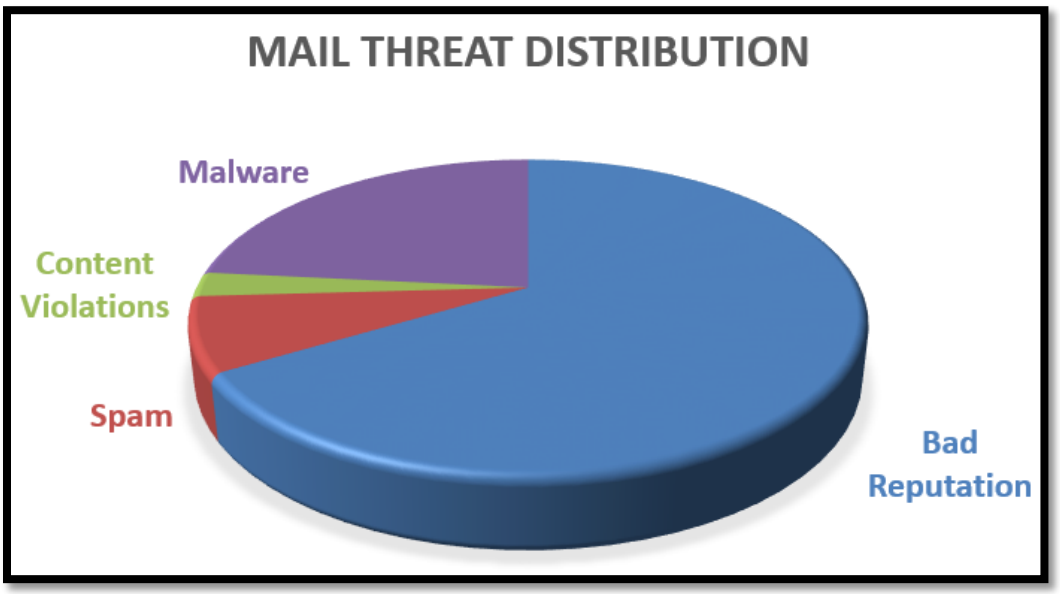


Picture 2: Application Exploits Distribution

Mail attacks

97 % increase in malware delivered via email over April

TruShield security analysts continue to witness an orchestrated effort to compromise corporate networks via email systems. Our SOC Analysts recorded a surge in the threats delivered thorough email systems. From the total incoming messages, 59 percent were determined as malicious, and as a result were blocked or deleted. To compare this statistic, during month of April we recorded only 47 percent of emails were malicious. Below is a current breakdown in the mail threat distribution.



Picture 3: Mail Attack Vector in Across All Industry

What is important to note is that in comparison with April, our incident responders had to deal with double the amount of malware delivered via enterprise mailing systems.

Cyber Threat Mitigation

Most of today's organizations handle a massive amount of personally identifiable information (PII), financial information, and intellectual property. If these companies were to rely solely on the traditional approach of security based on anti-virus solutions and perimeter firewalls, their data could quickly become a toxic asset. Moreover APT, zero-day vulnerabilities, and polymorphic malware - or one without available signature - threats cannot be stopped by static network defense.

TruShield's unique approach in mitigating cyber threats goes well beyond the majority of Managed Security Services Providers. Our organization combines state-of-the-art Continuous Security Monitoring with Defense-in-Depth and Zero-Trust network architecture. Offered as a complete solution or tailored one, TruShield's adaptive security offering is one of the most effective approaches that allows our clients to consequently block and deter botnets, APTs, new malware, and malicious insider threats. Finally, our strategy tends to disrupt the Cyber Kill Chain in its earliest phases, reconnaissance.

Another key element in mitigating and managing cyber risk is TruShield's extensive expertise in vulnerability management and disaster recovery solutions, which allows security architects and incident responders to apply real-world solutions in preventing, securing and - when the case requires - restoring its clients critical systems. Moreover, TruShield does not only strive for implementing security measures to ensure compliance but to exceed regulatory requirements.

References

https://isc.sans.edu/diary/Exploit+kits+%28still%29+pushing+Teslacrypt+ransomware/19581
http://www.eset.com/int/about/press/articles/malware/article/linux-and-bsd-web-servers-at-risk-of-sophisticated-mumblehard-infection-says-eset/
https://www.us-cert.gov/ncas/alerts/TA15-105A
http://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
http://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise/ransomware-on-the-rise
http://blog.checkpoint.com/2015/04/20/analyzing-magento-vulnerability/
http://www.oracle.com/technetwork/topics/security/alert-cve-2015-3456-2542656.html

TruShield Security Solutions

TruShield is a leading provider of Managed Security Services across the globe. We are dedicated to helping companies achieve success by making sure they are properly prepared against the current and emerging threats in today's digital world. Our service offerings include: Continuous, 24/7/365 Monitoring, Penetration Testing and Vulnerability Assessments, Audit and Compliance, and many other Managed Services such as Managed Firewalls and Hosted Log Management. We also offer Security Awareness Training and Management Consulting services.

Contact us today to find out how we can help you protect your organization and safeguard your information.

Contact Information:

Email: support@trushieldinc.com
Web: www.trushieldinc.com
Phone: (877)-583-2841

Follow us on:

TruShield Blog: http://trushieldinc.com/blog
Twitter: @trushield
LinkedIn: https://www.linkedin.com/company/trushield-security-solutions
Facebook: https://www.facebook.com/trushieldinc