Fortify Your Network Protection with Actionable Intelligence using *Today's Top Threats*

White Paper/April 2014

Malcovery Security's Today's Top Threats™ report provides your information security team with in-depth intelligence about emerging threats that pose an imminent danger to your enterprise network.

It started simply enough when a small group of HR employees at RSA, the Security Division of EMC Corporation, received an email message entitled "2011 Recruitment Plan." The company's spam filter must have determined that something wasn't quite right about that particular message because it was delivered into the recipients' junk mail folder. Nevertheless, at least one person retrieved and opened what was in reality a spearphishing message. The unaware employee then clicked on the attached Excel spreadsheet which, unfortunately, had been compromised with the recently-discovered Adobe Flash zero day flaw (CVE 20110609).

This unleashed a malware Trojan onto the enterprise network that proceeded to harvest login credentials within the RSA network. The malware eventually helped the attacker obtain privileged access to the targeted system, where highly sensitive data and files were stolen and sent to an external compromised machine at a hosting provider. At this point RSA information security (InfoSec) professionals noticed the attack happening and stopped it to prevent further damage—but not before the attacker stole information specific to RSA's SecurID two-factor authentication products.

Over the course of the next 3 months, EMC spent $66 million dealing with the fallout from this breach and theft of critical and highly sensitive intellectual property, according to the company's Chief Financial Officer.[1] This figure doesn't include the cost of investigating the attack, hardening RSA's systems to prevent further intrusions, and working with customers to prevent their being exploited as a result of the attack.

If an incident like this can happen to one of the world's leading IT security vendors, it can happen to practically any organization. It's probably safe to say that RSA, like every other conscientious enterprise, has a variety of security controls in place: firewalls, spam filters, anti-virus/anti-malware, IDS/IPS, web gateways, blacklists, whitelists, URL blocking tools, sandboxes, a SIEM, and so on. But these tools are only as effective as the policies they operate under and the intelligence that is fed to them.

This white paper discusses how you can use actionable threat intelligence about the most serious email-borne threats that are affecting your network today. And we mean that quite literally when we say "today." Malcovery's Today's Top Threats report provides the specific intelligence you need to make your existing security controls more effective and your InfoSec team smarter.

[1] InformationWeek, "RSA SecurID Breach Cost $66 Million," July 28, 2011

Don’t let your enterprise be the “wheat”

RSA isn’t the only company to have suffered terribly from an attack that originally stemmed from someone opening a malicious email. The same vector was used to open the door for the notorious 2013 attack on Target Corporation resulting in data loss affecting 110 million customers. Security reporter Brian Krebs wrote on the KrebsOnSecurity blog[2]:

> *The breach at Target Corp. that exposed credit card and personal data on more than 110 million consumers appears to have begun with a malware-laced email phishing attack sent to employees at an HVAC firm that did business with the nationwide retailer, according to sources close to the investigation.*
>
> *Last week, KrebsOnSecurity reported that investigators believe the source of the Target intrusion traces back to network credentials that Target had issued to Fazio Mechanical, a heating, air conditioning and refrigeration firm in Sharpsburg, Pa. Multiple sources close to the investigation now tell this reporter that those credentials were stolen in an email malware attack at Fazio that began at least two months before thieves started stealing card data from thousands of Target cash registers.*

Krebs further speculates on why Target’s third party vendor was in the crosshairs for the malicious email:

> *Many readers have questioned why the attackers would have picked on an HVAC firm as a conduit for hacking Target. The answer is that they probably didn’t, at least at first. Many of these email malware attacks start with shotgun attacks that blast out email far and wide; only after the attackers have had time to comb through the victim list for interesting targets do they begin to separate the wheat from the chaff.*

Unfortunately for Target Corporation, they were identified as wheat and not chaff.

There are too many phishes in the sea

It’s astounding to think that so much damage can result from malicious email. Even one person taking the bait of a phishing message that unleashes malware within an organization can lead to millions of dollars in damages—yet this is something that happens every day.

Consider these statistics from the Anti-Phishing Working Group (APWG) and several prominent security vendors:

- More than 30 billion spam messages are sent every day.[3]
- About 65% to 70% of all inbound email is spam.[4]
- 156 million phishing emails are sent every day.[5]

[2] Brian Krebs, “Email Attack on Vendor Set Up Breach at Target,” February 14, 2014
[3] Symantec Corporation, “Symantec Internet Security Threat Report 2013”
[4] Various sources, including Trustwave SpiderLabs Services, Kaspersky Lab, Symantec Corporation
[5] Symantec Security Technology and Response Group, August 2012

- About 16 million phishing emails make it through defense systems intended to block these types of messages. Of these, 8 million are opened; 800,000 links are clicked; 80,000 people fall for the scam, providing confidential account credentials or other information to a spoofed website or downloading a malicious payload.[6]
- In 2012, 1 in 291 email messages linked to malware on the Internet or had malware attached to it.[7]
- There were more than 200,000 phishing attacks (campaigns) worldwide in 2012. More than 150,000 unique domain names were used in these campaigns. More than 600 brands (i.e., company names) were abused in these campaigns. PayPal was cited as the most frequently abused brand in 2012.[8]
- Global losses from phishing were estimated conservatively at $1.5 billion in 2012—a 22% increase over losses in 2011.[9]

As you can tell from these numbers, the odds of having malicious emails end up within your enterprise are certainly not in your favor. Vast new spam and phishing campaigns are unleashed every day. The interesting thing is that many of them can be traced back to just a few bad actors. Research conducted by Malcovery Security shows that a single attacker can be responsible for sending out millions of messages a day. Malcovery Security has engineered a way to exploit this fact to provide you the threat intelligence necessary to block these attacks when they are in their earliest stages—perhaps even before they come knocking at your door.

Traditional security controls are struggling to keep malware out

Email attacks are a primary mechanism to deploy malware into enterprises, either directly or indirectly. Of the 47,000 data breaches investigated or analyzed by the Verizon RISK Team in 2013, 67% of the time in large enterprises, email was the direct vector. And still more often, malicious email was the mechanism by which bad guys gained access to a computer and then directly installed malware on it.[10]

What's the difference between Phishing and Malware?

The relationship between phishing and malware is a bit blurry, mostly because they often work together to achieve the goal of the cybercriminal. In fact, the term "malware" is often included in phishing discussions. Now that being said, here is Wikipedia's malware definition:

"Malware, short for malicious software, is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software."

"....Malware includes computer viruses, ransomware, worms, Trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs, rogue security software and other malicious programs; the majority of active malware threats are usually worms or Trojans rather than viruses...."

One key distinction is that not all malware is delivered via email. Malware converges with phishing when it is being used as an accessory to execute the phishing attempt.

[6] Canadian Government website www.GetCyberSafe.ca, "Phishing: How Many Take the Bait?"
[7] Symantec Corporation, "Symantec Internet Security Threat Report 2013"
[8] Anti-Phishing Working Group, Global Phishing surveys, 1H2012 and 2H2013
[9] RSA, the Security Division of EMC, "2013 Fraud Report"

Every sizable organization with a network to protect has implemented a range of solutions designed to keep email-borne malware out—or at least to prevent or minimize damage if it does get delivered to in-boxes. Unfortunately none of these solutions has proven to be 100% effective. The porous protections, particularly those at the network perimeter, are struggling to keep up with new evasion techniques that clever cyber-criminals develop to circumvent existing controls.

Here are just a few examples of the shortcomings of defenses companies rely on every day to keep their networks safe:

- **Anti-virus / anti-malware** solutions are almost always trailing behind the current types of viruses, Trojans and malware because they are dependent upon the vendor developing a signature to detect the presence of the malicious code. Viruses and malware are so plentiful – a million new, unique malware samples a week are submitted to AV-TEST[11] – that many AV vendors wait until a "critical mass" of incidents are recorded in the wild before writing and distributing a signature to prevent further infections. In a recent study by Malcovery's research partner, the University of Alabama at Birmingham, the average AV industry detection rate for Today's Top Threats malware is 17%, meaning that 83% of current anti-virus solutions would fail to detect the top malware campaign delivered by spam on any given day.

- **Appliances** such as firewalls, proxies, gateways and filters all work on rule engines. Cyber criminals have learned how to skirt many of the rules that security analysts utilize. For example, an attacker will spoof the "sender" address to match one that appears to be legitimate and is likely to be on an approved whitelist; for example, statements@MyBank.com. In the phishing email, the spammer will say something to the effect of "Please add this to your address book to make sure that you never miss a statement from us." Once that address is on the whitelist, email from that sender address will sail through defensive filters untouched. Attackers know this and they craft their malware-laden messages so they appear to come from senders that are in people's whitelisted address books.

Blacklists can be circumvented as well. You must know what is bad to prevent access to it. Attackers get around this defense by corrupting and using virgin websites and IP address, etc. to launch an attack, and then abandoning them after a few hours once their damage is done. To be clear, blacklists can be an effective part of a good defense, but only if they are fed timely and actionable intelligence.

For every type of rules-based appliance, the rules need to be kept up to date with the best information to prevent threats yet allow valid transactions.

[10] Verizon RISK Team, "Verizon 2013 Data Breach Investigations Report," April 2013

[11] Andreas Marx, AV-TEST, in "Experts Slam Imperva Antivirus Study," January 23, 2013

- **Sandboxing** is an effective way of detecting malware that comes in through a network perimeter. A suspicious file can be thrown in a sandbox and forced to run to see if it's harmful. However this technique isn't able to catch infections that occur when a user's device is off the network. A worker takes his laptop home, opens his personal email and gets an infection. When he brings that compromised device back onto the enterprise network, the malware can be unleashed to do its harm.

- **Endpoint software** is difficult to deploy and maintain. Heterogeneous environments and the growing practice of bring-your-own-device (BYOD) complicate platform support and management. And due to limited battery life and device memory, smart phones and tablets do not support endpoint software effectively.

We would never suggest that you not use these and other network defenses. They do play a vital role in securing your network, even if they have their individual shortcomings. Their efficacy can be raised, however, when given the right kind of intelligence that has an immediate impact on network security.

A new approach to security intelligence is needed

Malcovery Security takes a fundamentally different approach to understanding attacks that begin through malicious email campaigns. We believe you need to know your enemy to understand how he or she is going to attack you. Therefore we focus our resources on who is behind these campaigns, what infrastructure they are using to do their dirty work, and how to block or mitigate their attacks on your network. We call this process adversary analysis.

Malcovery has an extensive and continuously growing database of confirmed phishing sites and the infrastructure that spammers use to send their messages and collect responses from victims who fall prey to the attacks. We use an arsenal of public and proprietary tools to investigate and visualize the origins of these attacks. As we conduct this analysis each day, we see that just a few people are behind the largest attacks.

Figure 1 below illustrates how some of the different campaigns that we look at every day are related. The graphic shows a couple of black hat guys and each one of them represents a different company whose brand was spoofed – for example, various banks, package delivery services, and so on – and lots of messages were sent out using those brand names throughout the day. Some of those messages are sent out with attachments that are malicious and others contain links inside to drive-by malware.

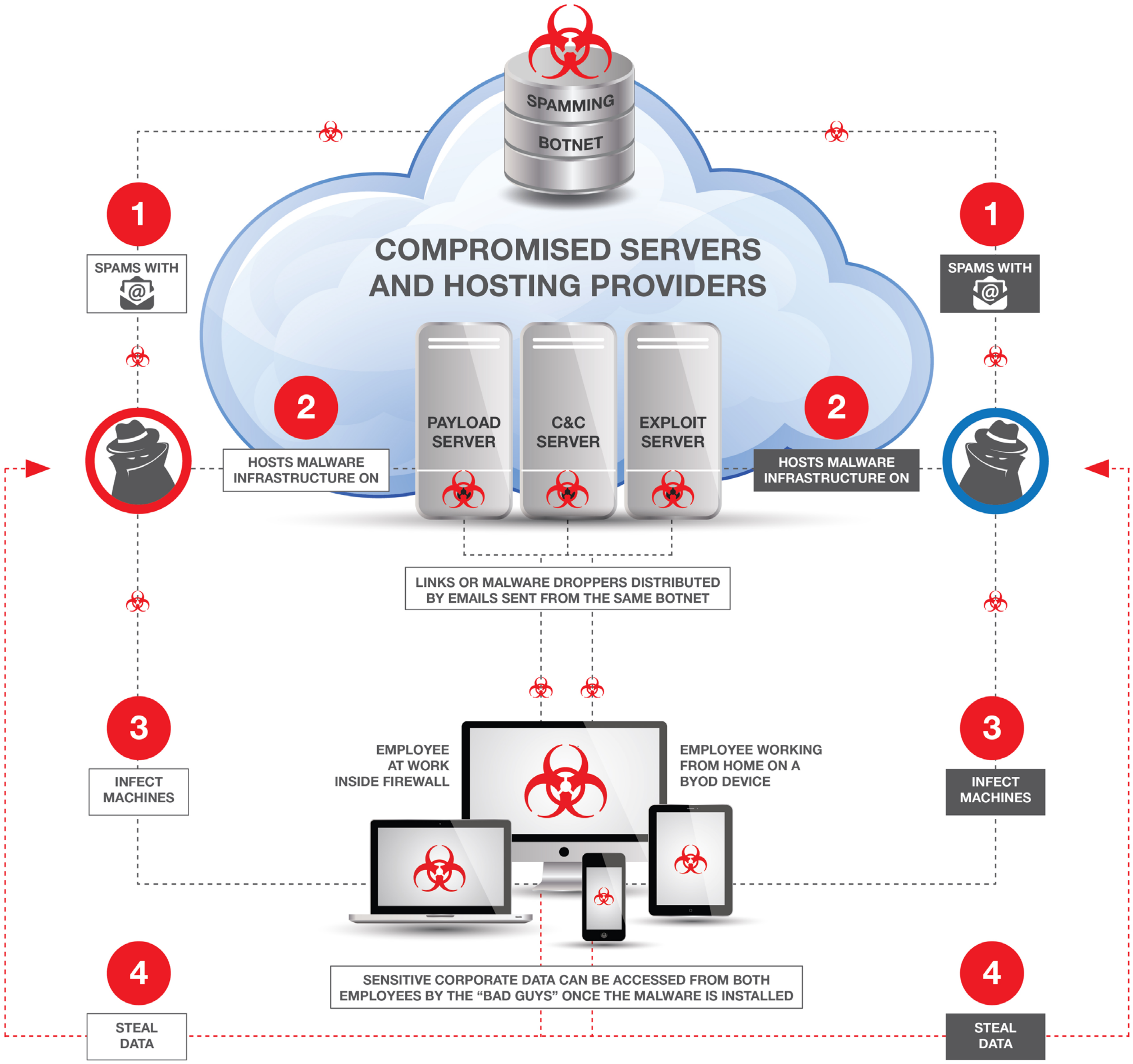
SPAMMING
BOTNET
COMPROMISED SERVERS AND HOSTING PROVIDERS
1
SPAMS WITH
1
SPAMS WITH
2
HOSTS MALWARE INFRASTRUCTURE ON
PAYLOAD SERVER
C&C SERVER
EXPLOIT SERVER
2
HOSTS MALWARE INFRASTRUCTURE ON
LINKS OR MALWARE DROPPERS DISTRIBUTED BY EMAILS SENT FROM THE SAME BOTNET
3
INFECT MACHINES
EMPLOYEE AT WORK INSIDE FIREWALL
EMPLOYEE WORKING FROM HOME ON A BYOD DEVICE
3
INFECT MACHINES
4
STEAL DATA
SENSITIVE CORPORATE DATA CAN BE ACCESSED FROM BOTH EMPLOYEES BY THE “BAD GUYS” ONCE THE MALWARE IS INSTALLED
4
STEAL DATA

Figure 1 – Network analysis of the sources of large volumes of spam/phish on a single day

This graphic illustrates that whether it is a link campaign or an attachment campaign, or the spoofed brand was Wells Fargo or FedEx, all those pieces of malware were reaching out to a common distribution infrastructure. We know that the criminals use that common infrastructure day after day, week after week. They use the FedEx brand this morning and Wells Fargo this afternoon and the malware may be slightly different but it’s going to be communicating with and connecting to those same command-and-control servers and the same IP addresses and URLs. We want our customers to block them now because we know the criminals use those same resources again later.

The most commonly reused resources are:

- **Spamming botnet** – Malicious links and malware droppers are distributed by emails sent from the same botnet.
- **Compromised domains or hosting providers** – Compromised domains and hosting providers are ripe with malware payloads or exploit sites
- **Infected machines** – Machines infected with malware of the same type communicate with a single, large, multipurpose botnet and are often used to distribute malware

What we can learn from analyzing large spam campaigns

Let's take an in-depth look at what can be learned by analyzing some of the largest spam campaigns executed on a particular day.

Over the time span of February 4th through the 7th, 2014, Malcovery observed a number of very large spam campaigns utilizing numerous malicious attachments. These attacks were some of the most prolific, persistent and advanced threats that we have analyzed. They showed evidence of a very capable adversary with ample resources at hand, impersonating more than five well-known brands and distributing numerous unique malware samples. The volume of the spammed emails was staggering, as was the ability of the attacker to diversify the set of malicious attachments distributed by the emails. However, the attacker utilized the same resources for hosting command and control resources as well as payloads to be distributed to victims' machines—a characteristic which allowed Malcovery's analysts a great deal of insight into the attacker's infrastructure.

We found that over this four-day period, two IP addresses were utilized in each day's attack, each belonging to a distinct ASN (autonomous service number indicating a specific grouping of IP addresses). (See Figure 2.) This is a strong indication that the same party was responsible for all of these spam campaigns. Furthermore, referencing historical data collected from all of Malcovery's Today's Top Threats analyses indicated that IP addresses on the same ASNs had been used previously to distribute very similar malware.

Figure 2 – Relationships observed among spam campaigns, February 4 – 7, 2014

Brand used in the email to trick recipients	The way the IP was used in support of the attack	IP Address	ASN	Date Used
RingCentral; Lufthansa	C&C	85.143.166.167	AS56534	11/13/13
Skype; DHL	C&C	85.143.166.215	AS56534	11/26/13
Bank of America	C&C	85.143.166.119	AS56534	2/5/14
Visa; MasterCard	C&C	85.143.166.119	AS56534	2/6/14
FedEx	C&C	85.143.166.119	AS56534	2/7/14
Expedia; Vodafone	C&C	62.76.187.113	AS57010	8/1/13
Expedia; Vodafone	Payload distribution	62.76.187.147	AS57010	8/1/13
Various ISP	C&C	62.76.187.171	AS57010	2/4/14
Bank of America	C&C; Payload distribution	62.76.187.171	AS57010	2/5/14
Visa; MasterCard	C&C; Payload distribution	62.76.187.171	AS57010	2/6/14
FedEx	C&C; Payload distribution	62.76.187.171	AS57010	2/7/14

This analysis yields two major elements of threat intelligence:

- Upon identifying and analyzing the first of the February 2014 attacks, Malcovery provided our customers with actionable intelligence they could use to protect themselves from the subsequent malware distributions on the following days. This is important in the immediate timeframe of an attack in which rapid response is crucial to protecting one's network and organization.

- Coupling prior use of IP addresses on the same ASNs with use of the same malware type provides a strong indication that the same party perpetrated all of these attacks. This observation provides savvy security professionals with valuable information about how an attacker works, allowing those professionals valuable heuristics for designing a response to similar attacks in the future.

The intelligence Malcovery provides allows for network security architects to populate their firewalls or web proxy's filters with known bad locations. This action can nullify a malware's ability to interact with its command and control resources which are often shared among a number of attacks. Thus the savvy security professional can prevent communication with the root of not just one malware sample's infrastructure but potentially many more. Furthermore, Malcovery's reporting of traits shared among the spammed emails – such as repeated use of a finite list of sender domains, commonalities among email message headers, or use of identical email content – affords email security specialists the ability to more effectively identify hostile messages as they cross into an organization's environment and deny an attacker that vector into an organization.

Additionally from the example above, searching historical phishing data indicates that the ASN 56534 was observed as hosting two phishing pages in 2012. While not a strong correlation with the malware attacks analyzed in the past year, it is notable that resources have been shared in this way. At this point the reputation of the hosting provider can be flagged. A hosting provider which allows malware to be distributed from their servers and allows phishing sites to operate from the same resources can be held in low esteem and warrant scrutiny when seen in network communication. The same might be said for legitimate sites that are compromised for nefarious purposes. If malware is observed on the site and then cleaned, the underlying vulnerability may still exist and be leveraged by criminals to carry out more hostile activity.

Protect your network from the top threats of the day

Each day Malcovery analysts scour the Internet for emerging threats in the form of emails that contain links to malicious websites or that contain malicious attachments. Characteristics about the spam messages and the associated malware are documented in a daily report called *Today's Top Threats*, or T3 for short. The report actually takes two forms: a "human-readable" report in PDF format and a "machine-readable" report in XML or STIX format. (STIX is an industry standard format developed by Mitre Corporation for sharing structured cyber threat information. The STIX Campaign definition provides a rich set of data for related threats.)

The T3 product utilizes the Malcovery Spam Data Mine which receives more than a million spam messages each day from a wide variety of sources. Clustering algorithms analyze the spam on a number of factors and watch for "emerging threats" in the form of emails that contain links to malicious websites or that contain malicious attachments. Once a new Threat Cluster is identified in the spam, characteristics about the spam messages and the associated malware are documented.

The PDF file makes your InfoSec team smarter

Issued at least once a day, the PDF version of T3 gives your InfoSec team information it can use in so many ways. This report typically describes the threat in terms of:

- The subject lines used in the spam messages
- The message content (what an end user would see)
- The sender domain, which is often spoofed or hijacked
- What the malicious link or attachment does
- How many anti-virus products detected the malicious binary
- The hash of the binary
- What IP addresses and/or URLs are used in the attack
- The indicators of compromise (IOCs) if the malicious attack gets into your network
- Malcovery's expert analysis of the attack methodology

Additional information is added as it is relevant to a specific campaign or attack.

Here are some common use cases Malcovery customers have for the PDF version of T3.

- An email security analyst sees what mass email campaigns might be directed toward the organization that day. From the T3 report he can see what subject lines and sender domains are associated with this spam, and he can block these messages before they go into users' in-boxes. He can search for these attributes in users' in-boxes to see if anyone received the message already and, if so, retract it if it's unopened. If the message has been opened, he can issue a trouble ticket to have the user's device quarantined and remediated, and then initiate an incident report to look for the IOCs on the network.

- A security analyst searches through logs, or perhaps a SIEM, to see if there has been any traffic going out to known bad websites or reaching out to a command-and-control server. When such instances are found, she can trace which devices initiated those actions and, like the example above, issue a trouble ticket to have the devices quarantined and remediated, and then initiate an incident report to look for the IOCs on the network.

- An employee clicks on the wrong attachment at work and this results in a dropper being installed on his laptop. The dropper tries to connect to the payload site but it's blocked at the proxy because it was an adult website. Even though the action was blocked, the InfoSec team would want to know that this PC is trying to communicate with a malicious server. The company can use a product like Palantir to look for the intersection between known malware sites that Malcovery provides and outbound communication though the proxy. Then Palantir can alert the InfoSec team, who could initiate remediation of the PC or even disable the user's network access using Network Access Control (NAC) technology if they have it deployed.

- An organization that does end user security awareness training can use examples of real attacks to educate its users on what is happening today. If the company uses a phishing simulation tool like PhishGuru[12] or PhishMe[13], the trainers can use a replica of these real phishing messages in a controlled environment to see if employees are likely to take the bait, and if so, provide additional security training.

- The team responsible for security awareness can issue alerts inside and outside of the organization to let employees and customers know about specific, credible attacks they should watch for. For example, a bank can proactively warn its customers about known phishing attempts, including what the messages look like, in order to prevent customers from becoming victims.

[12] PhishGuru is a product of Wombat Security Technologies
[13] PhishMe is a SaaS offering from PhishMe

The XML/STIX files improve the effectiveness of your security infrastructure

While the detailed PDF file is published once a day, the machine-readable file is updated numerous times a day, as new campaigns are verified. Using the MRTI, the InfoSec and Incident Response teams can automate many of the actions they perform based on the daily report to achieve greater efficiency. All of the machine-readable threat intelligence (MRTI) is accessible via secure FTP and be quickly imported into Web proxies, secure gateways, IDS/IPS, firewalls or web filter protection services to guard your network.

By importing immediate, current data into these devices, they are able to detect and block emerging threats at the earliest stages of attack. Moreover, because we know that cyber criminals reuse their attack infrastructure for days, weeks or even months and for a variety of campaigns, blocking access to the URLs and IP addresses that Malcovery identifies today will protect your organization for months to come.

Here's an example of how the XML or STIX file can be used:

- A programmer for an enterprise organization writes a short script for a routine that goes to the Malcovery server, checks the T3 index file to see if there are any recent updates, fetches the new data, identifies the XML tags within it, creates a file update and uploads it to a web filtering device. This routine is run repeatedly throughout the day to ensure that the web filter has all of the new information published by Malcovery. These updates prevent traffic flowing through the filter from reaching out to known malicious sites.
- Many organizations will feed MRTI directly into their SIEM which will correlate the intelligence with other types of data to produce timely and reliable input to the threat detection and policy enforcement components of their security infrastructure.

The benefits of using Today's Top Threats to protect your infrastructure

The combination of the two forms of the T3 report – human and machine-readable – can help you provide better protection for your network.

- **Get critical, actionable intelligence faster.** Learn what email-borne threats are active today, now. Use the information to block users' access to malicious email messages and harmful URLs before they click to open or access them.

- **Get broader coverage and stronger protection from threats.** Integrate the intelligence from T3 into your existing security infrastructure to automatically fortify your defenses as soon as threats are detected.

- **Learn the indicators of compromise.** T3 can tell you exactly what to look for within your network to determine if an infection or active attack is underway so that you can remediate the problem sooner.

- **Get proactive protection against future attacks.** By blocking access to the known malicious infrastructure reported in T3, you can protect your network from future attacks that can be expected to use that same infrastructure.

- **Get more value from your existing security infrastructure.** T3 information is a complement to your existing defenses. Get better ROI from the tools you already have deployed.

- **Use real scenarios in your security education programs.** As phishing and spearphishing campaigns use social engineering lures that are more believable, your end users are more likely to fall for them. Use the real scenarios that are provided in T3 to train your employees to avoid becoming victims.

- **Provide better customer service through security awareness and outreach.** Proactively inform your end users about threats they may encounter to help them be more security-aware.

- **Improve situational awareness.** Mature security organizations with Threat Intelligence and Incident Response programs can leverage the advanced context Malcovery provides about malware campaigns through integration with visualization software like IBM I2 and Palantir and as input to cyber kill chain framework.

Get started—put Today's Top Threats intelligence to work for you

If you are responsible for protecting your network or email system from cyber criminals and would like to learn more about how Malcovery Security can help you, visit http://info.malcovery.com/fortify-your-network-protection-with-actionable-intelligence-using-todays-top-threats and request a demonstration of how T3 intelligence can improve your security posture.

About Malcovery Security

Malcovery Security is the leading provider of actionable cyber security intelligence and forensic analysis about email-based threats (phishing, spam and malware) that identifies, prioritizes and targets cybercriminal activities and provides effective countermeasures.

Delivered as a suite of subscription services, the company's patented and patent-pending technology provides the ability to identify the root sources of cybercrime attacks (servers, perpetrators, locations, etc.), delivering rich actionable intelligence information about cross-brand attacks and targeted attacks, as well as advanced notification of emerging email-based threats.

Unlike services that serve only as a reactive response to these attacks today—services that simply address the symptoms but cannot provide the intelligence to actually stop the cybercriminal and their activities—Malcovery Security's solutions provide the unique intelligence required to respond effectively to attacks on customers' brands, to disrupt email-based threats on an organization.

Malcovery Security has offices in Pittsburgh, PA and Birmingham, AL.

For more information, please visit http://www.malcovery.com or connect with Malcovery on Facebook (facebook.com/malcovery), Twitter (@malcovery), and LinkedIn (http://www.linkedin.com/company/malcovery-security).