MALCOVERY SECURITY

Closing the Window on Losses to Phishing

White Paper/April 2013

When phishing web sites are launched, the clock starts ticking as your customers' credentials are stolen by cyber-criminals. The window of time between the establishment and proliferation of phishing sites and remediation is critical and must be lowered to reduce fraud losses.

Malcovery Security has licensed the technology developed by world-renowned phishing experts at the University of Alabama at Birmingham (UAB) to identify and track phishing intelligence in the most comprehensive way. Malcovery phishing intelligence goes beyond the standard takedown process to pro-actively protect your brand, using patented techniques and cross-brand intelligence. *By engaging Malcovery, you will reduce the attacks on your brand over time, and you will create and enforce a lasting deterrent to cyber-criminals, all while significantly reducing short-term fraud losses.*

The Open Window

The response to phishing for most companies is to engage a specialized vendor to outsource the tricky business of phishing site takedown. But even though some vendors have been very successful in cutting down the amount of time it takes to have a phishing site removed from the Internet[1], these vendors are not capitalizing on all of the information available to them.

The Malcovery process employs techniques honed over years of highly-specialized research and enormous amounts of collected data. This data includes the Internet location (URL and IP), whois and reputation information about the domain name and IP, and copies of all the component files of the web site — all of this for hundreds of thousands of phishing web sites that target hundreds of brand names.

One of the earliest and most compelling phishing research findings at UAB was that the majority of spam campaigns for disseminating a link to a phishing web site do not even last two hours[2]. The most prolific phishers spam out the link and then move on to their next spam campaign for sending out another phishing link. Because fraudulent web sites are easy and inexpensive to configure, phishers create up to hundreds each day. During the time it takes for the sites to be discovered and taken down, your customers are opening their email messages and clicking on the links within the messages to log in to what they think is your network. This is the timeframe during which authentication credentials are stolen. Most credentials are stolen during the first four hours that a phishing site is live.

---

[1] The Anti-Phishing Working Group (APWG) reported that, at the first half of 2012, the median phishing uptime had dropped to five hours and 45 minutes. See "Global Phishing Survey: Trends and Domain Name Use in 1H2012" available at http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2012.pdf

[2] Sheng, S., Wardman, B., Warner, G., Cranor, L.F., Hong, J., and Zhang, C. An Empirical Analysis of Phishing Blacklists. *CEAS 2009 – Sixth Conference on Email and Anti-Spam* (Mountain View, CA, Jul 16-17, 2009). http://ceas.cc/2009/papers/ceas2009-paper-32.pdf

Two other very important research findings at UAB concerned the analysis of phishing **Kit Files** and of the set of **Site Component Files** use to create the look and feel of a phishing web site. UAB automated the forensically-sound archive process for the software tool kits that criminals use to create phishing web sites. It is in the tool kits that the criminals' own email addresses are found, and knowing the email address that is receiving the stolen credentials is key to further investigation and to correlation with other phishing web sites created by the same criminal. Kit Files contain that particular email address but often contain other, hidden email addresses that belong to a different criminal or criminal gang involved in creating the software that comprises the kit and in distributing it to the frontline phishers. UAB knows how to find the hidden email addresses in phishing kits and has added these hidden addresses to its data mine about phishing. Knowing the email addresses of the kit creators allows additional correlation among the hundreds of phishing sites seen each day.

Being able to access, analyze, and archive the Site Component Files is also extremely important in the effort to reduce the amount of time it takes to automatically recognize a web site as fraudulent AND to automatically determine which brand name is being spoofed and victimized on the phishing web site. By using prior knowledge of which stolen corporate images are being displayed on the web site and which other known fraudulent sites have been created with the same or a similar set of component files, Malcovery can tell you *more and sooner* than any other provider.

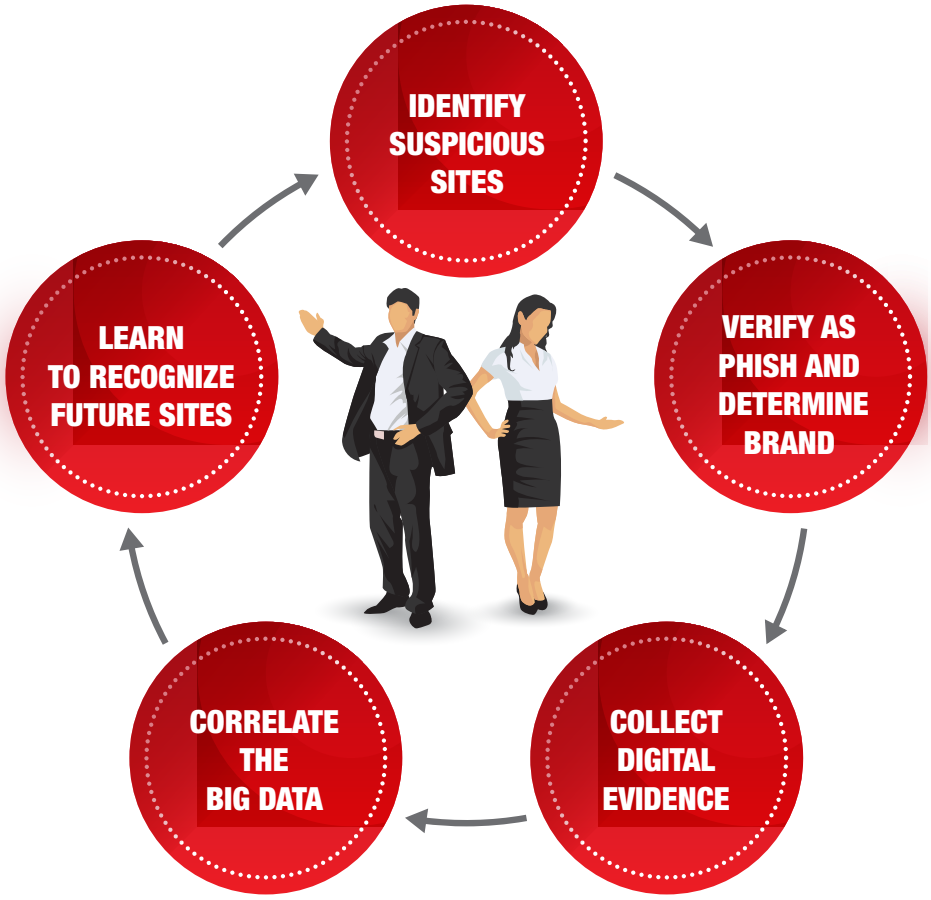
The Old Way

Take a look at the typical approach to anti-phishing that involves simple, reactive takedown:

Several minutes to hours may pass between steps 4 and 5. In the typical approach to anti-phishing, this is the window that must be lowered in order to reduce the number of credentials stolen, with the goal of reducing the fraud losses that your organization experiences. However, nothing about this process is pro-active, and it ignores the available digital evidence of the crime.

The Malcovery Way

Compare the above reactive process to the *pro-active* practice of creating actionable intelligence toward reducing fraud losses. Malcovery recognizes the need for a holistic approach to phishing that seeks out and verifies phishing sites using many available sources, collects all forensic information, and uses computer science techniques to correlate all of the data.



The first element of this process — **identifying sites as suspicious** — is extremely successful and discovers hundreds more phishing sites each day than are otherwise known. For example, your organization may collect information from a handful of sources regarding suspected phishing web sites, but this is done in a reactive way. Malcovery actually goes hunting for such sites by collecting not only from the traditional sources but also thoroughly collecting the original spam messages that disseminate the links to the sites. Again, using state-of-the-art software, Malcovery extracts the links and analyzes them in real time. Another hunting ground is on the servers of other phishing sites, and the Malcovery process checks several places on compromised servers to reveal other phishing sites.

These methods and other proprietary methods that cannot be disclosed allow Malcovery to out-perform takedown vendors in the first step, by producing a more complete[3] list of phishing sites.

The second element involves **verification of the suspected sites** as fraudulent and determining which online service provider brand is being spoofed. While there are several methods for doing this, the techniques that have been developed by Doctoral candidates and other computer forensics Graduate students at UAB have out-performed previous methods. UAB became aware very early in its research process that it would be crucial not only to provide an automated way to label a site as a phish but also to provide a highly-accurate way to determine which brand was being spoofed in a phishing attack.

Because Malcovery's labeling process is so fast and accurate, the takedown process can start much earlier. When Malcovery identifies phishing sites targeting your brand, your takedown vendor is notified immediately, keeping you ahead of the clock and saving your internal team the time and personnel costs of visually verifying phishing sites. And with early and accurate warning, your anti-fraud staff can also respond more efficiently, injecting incident intelligence back into your own systems and allowing a comprehensive understanding of the level of fraud losses for a particular criminal. Our experience has shown that the quick and accurate identification of related losses is necessary when referring a case to law enforcement.

Meanwhile, all of the **digital evidence is collected** in a forensically-sound manner. In the Malcovery phishing intelligence process, all of the files used to create a phishing web site that are being hosted on a fraudulent location (either the phisher's own host or a compromised host) are downloaded to Malcovery servers and archived. A unique identification number is assigned to each phishing incident, and all of the components of the incident are recorded, including the unique MD5 hash value for each component file. Using these unique values, Malcovery can confirm the identity of each component file and also analyze it for distinctiveness. Many phishers re-use several files found elsewhere on the Internet, changing only a portion of the file as needed. A patented algorithm takes these files apart and determines which portions have been altered so that the files can be compared more accurately to files from other, known phishing sites. This type of analysis allows Malcovery to systematically assign a targeted brand to a phishing web site and provides to you and your company the most thorough volume of phishing intelligence available.

Phishers continue to steal with impunity until someone stops them

The final real-time element in the Malcovery phishing intelligence process is to **correlate the data** among all known phishing sites toward helping you prioritize your investigative dollars. Using sophisticated innovations in clustering techniques that have their genesis in the identification of hidden infections in hospitals, Malcovery provides immediate access to how each phishing site is linked to other phishing sites.

[3] For some brands, the Malcovery process reveals up to ten times more phishing sites than all other sources combined.

Malcovery Value-added and Intelligent Response

Malcovery's popular PhishIQ portal allows your team inside access to Malcovery's data mine of phishing intelligence, where you can search by domain name or other URL sub-string, by IP address or range of IP addresses, and by drop email address (the phisher's clear text address or the kit creator's obfuscated address). Subscribers to PhishIQ can see intelligence about phishing threats against all brands (with private information protected, of course), allowing your investigators and law enforcement to fully understand the history and risk factors associated with certain domain names, IP addresses, and hosting providers. For example, PhishIQ provides details of one particular domain name that has hosted 170 different phishing sites. How many times should you pay to shut down a phishing site when the more appropriate, enduring approach may be to help the webmaster remediate security flaws? This higher level of intelligence helps your team make decisions more quickly and more accurately, resulting in significantly better outcomes.

The example of a serial phisher also helps to demonstrate Malcovery's smarter approach to phishing. With the extensive data in Malcovery's phishing data mine, Malcovery can identify the most troublesome, repeat offenders that continually victimize your company and your customers. When this type of attacker is identified, you will want to respond differently than you normally would. Malcovery will follow through with a more aggressive strategy that would require, for example, contacting the webmaster and requesting server logs to determine the attacker's IP address. Inside your organization, you will be able to lock-down accounts that are accessing your network from the related phishing sites. Once you know more about your attacker, you are better at defending against them.

Comparison

As you can see, simple takedown ignores how easy it is for a phisher to set up another phishing web site as soon as you take one down. Phishers continue to steal with impunity until someone stops them. And if they already have a good infrastructure set up for cashing out of credentials on your brand, then they will continue to create low-cost phishing web sites that target your customers. The takedown-only strategy also cannot solve the problem of the open window for loss of customer credentials. Even as takedown companies expand and improve their reactions, as long as the phishers keep coming back, your organization will be playing an expensive game of Whack-a-Mole with phishing sites. And some of those moles never pop up for you if you are not receiving full information. Takedown companies are not successful in identifying the large portion of phishing sites, and they are physically unable to remove sites quickly enough[4].

[4] Moore, T. and Clayton, R. Examining the Impact of Website Take-down on Phishing. eCrime '07 - Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit (Pittsburgh, PA, Oct 4-5, 2007). http://www.cl.cam.ac.uk/~rnc1/ecrimephish.pdf

Malcovery's patented system for automated phish branding uses the zeros and ones of the files of a web site to tell us whether it is a phishing site and whether it is spoofing your brand. With that intelligence, Malcovery's artificial intelligence (AI) system "learns" to recognize future suspicious sites as phishing sites spoofing your brand. When sites are identified, they are referred immediately to you and/or your existing takedown vendor. A threat level is also identified, which allows you or your vendor to prioritize within a limited takedown budget, removing the most harmful sites first[5].

You can also use real-time intelligence to enhance your own real-time anti-fraud efforts. Knowing the IP addresses and domain names associated with current phishing sites allows your network administration the ability to block access from those locations. Referrer information can also be used to determine how a customer navigated to your site. And devices that are authenticating from malicious locations can be monitored for suspicious activity and required to provide stronger authentication.

Malcovery's AI-based system thereby lowers the window that represents the amount of time it takes to recognize a phishing site and have it removed from the Internet... the same window that your customers' credentials are flying out of.

Addressing the Longer-term Costs of Phishing

Immediate costs of phishing include the money you reimburse to compromised accounts and the fees that you pay your takedown vendor. The longer-term costs of customer alienation and brand erosion are harder to quantify but are on the rise. Even as you strive to close the window, phishing opens the door on the victim's machine to further identity theft. As described by veteran computer security expert Mike Rothman of Securosis in the research paper *Email-based Threat Intelligence: To Catch a Phish*[6], attackers are increasingly looking to maintain a presence on the victim's computer in order to further monetize the compromise. Therefore, it is better to reduce phishing overall even if it means a greater short-term commitment[7]. Organizations that have made this anti-fraud commitment have reaped the benefits of pre-emptive cyber-security efforts, and their customers are not forced to fend for themselves in cyberspace. An advanced approach to phishing will help to make your organization the preferred provider in today's competitive markets.

---

[5] The threat level may be based on the recognition of a new phishing kit, a new phisher, or the volume of visitors to a phishing site. Other situations that may cause a higher priority include the discovery of a large group of sites that involve similar kit or component files or phisher or kit creator email addresses, or a set of sites that are hosted in the same vicinity (such as fraudulent names created with the same registrar, or sites hosted on a close range of IP addresses).

[6] Available online at https://securosis.com/research/publication/email-based-threat-intelligence-to-catch-a-phish

[7] Nero, P., Wardman, B., Copes, H., and Warner, G. Phishing: Crime that pays. eCrime Researchers Summit, 2011. (San Diego, CA, Nov 7-9, 2011). http://thecenter.uab.edu/media//2011/12/Phishing-Crime-That-Pays.pdf

Saving Money, Saving Face, and Preventing Future Incidents

In summary, Malcovery's turn-key phishing intelligence service provides the following benefits for you:

- Identification of more of the phishing sites that are being created to victimize your customers.
- Accurate labeling of phishing sites according to spoofed brand.
- Capture and preservation of forensic data for the investigative and prosecution processes.
- Scientific correlation of the attack details with data from years of collected phishing evidence, including attacks on other companies.
- Predictive analysis for the identification of future attacks.
- Skilled personnel who recognize subtle but important changes in criminal attack methods.
- Actionable intelligence to enhance your existing anti-fraud measures.
- An anti-phishing solution that demonstrates your organization's commitment to information assurance.

Malcovery's intelligence-based approach to phishing reduces fraud losses and incident response costs — both near-time and in the future — and preserves and protects brand reputation and customer satisfaction and loyalty.