ELSEVIER

computer FRAUD & SECURITY

ISSN 1361-3723 September 2009

www.computerfraudandsecurity.com

Featured this month:

The need for a united industry in combating malware

Believing that net users deserve better than the prevailing no man's land of internet security, Melih Abdulhayoglu of Comodo has founded a forum where interested parties worldwide can come together to discuss security issues and problems within the industry.

Called the Common Computing Security Standards Forum (CCSS), participants such as security software vendors, operating systems vendors and browser vendors are all invited and membership is free of charge. Via teleconferencing and listserve, members can discuss solutions for issues such as malware and phishing. This summer, the organisation published its first list of legitimate anti-virus software packages.

The Forum hopes to play a key role in developing standards for malware detection, provide a communications channel between vendors, and also offer a link between the IT security world and other industries.

Turn to page 2...

The need for a united industry in combating malware

Melih Abdulhayoglu

Melih Abdulhayoglu, CEO and founder, Comodo

The internet offers so much potential for good that it distresses honest computer professionals to see thieves preying on internet users. This year, security vendors worldwide have banded together to combat online malware and phishing by creating the Common Computing Security Standards Forum (CCSS).

CCSS is a voluntary organisation of security software vendors, operating system providers and browser software creators, working together to mitigate the risk of malware, and protect consumers worldwide. Believing that internet users deserve better than the prevailing No Man's Land of internet security, I invited antivirus and browser companies to a preliminary meeting in March. We began to map out a strategy on how the industry as a whole could eliminate or mitigate the spread of malware. I feel that every qualifying vendor should join the forum (qualifying vendors being those that produce the products above and who are interested in working with other industry leaders in mitigating malware). Participation is free and consists of telephone conferences and a listserve where we discuss solutions to industry problems. Invited participants include:

1. Security software vendors: Key to the organisation are vendors that produce and distribute security software. The security products must not be OEM products of another provider nor rely strictly on downloading or using the signature files of another vendor.

2. Operating systems vendors: OS vendors are also invited because they have a specific interest in protecting their users from malware.

3. Browser vendors: These are key in stopping malware, as most viruses have the internet to thank for their dissemination. Web browsers unintentionally help malware spread faster by providing access to malware-infected sites. Only by working with browsers can vendors hope to stop the rampant spread of infestation. I'm particularly excited about finding solutions with browsers that stop malware at the source.

The main goals towards which I foresee the forum working include:

1. Developing standards in detecting and identifying malware.
2. Providing an avenue for easy communicaion about industry problems for vendors.
3. Being a point of contact with other industries that affect the current state of the industry.

Although some vendors disagree on particular points, all security vendors agree that internet users are under attack. As software proliferates and grows more sophisticated, identified vulnerabilities increase exponentially – from a few hundred 10 years ago to nearly 40,000 today (see Figure 1).

Over the summer of 2009, two significantachievements were made toward mitigating malware.

First, the CCSS published a list of legitimate antivirus software packages. The stakes are high here. All a cheat has to do is plant small pop-up messages warning users that their computers may be infected. Scareware and ransomware are hardly more sophisticated than Nigerian email scams, yet they can reap a scammer $10,000 a day.

The CCSS Forum established an innovative approach to stopping this rogue malware by creating a list of legitimate

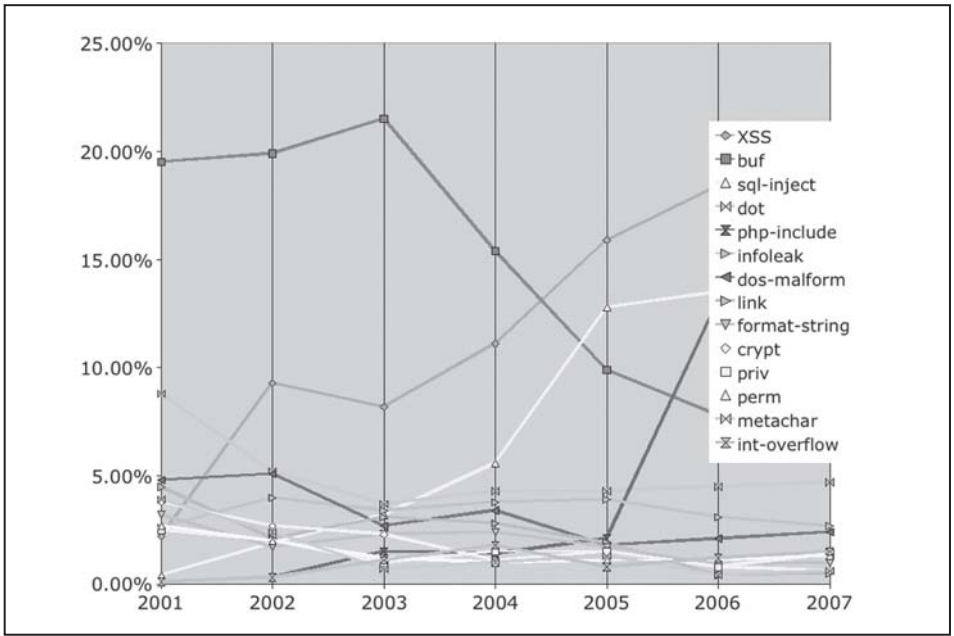

Figure 1: Common Vulnerabilities and Exposures (CVE) growth, September 1999 to August 2009. CVE is a dictionary of common names for publicly known information security vulnerabilities. http://cve.mitre.org/about/ Courtesy: The MITRE Corporation.

security software vendors.[1] Participants are not charged a fee for inclusion. Every security software developer may submit an application to the CCSS forum by emailing us at: questions@ccssforum.org. Every internet user considering new security software should check this list first before making a decision.

Second, the CCSS established a system for reporting digital certificates used by fraudulent sites or malicious code. One problem that Comodo sees, as a certificate authority, is that many malware companies and fraudsters feign legitimacy by using SSL certificates. They think this certificate can be used to camouflage their true intentions.

Previously, users had to request informationand to report certificates directly to the issuing certificate authority. How to do so is often not very clear. For example, many users may not realise that a certificate marked 'UTN-USERFirst' is actually a Comodo certificate. If they find malware and want to report its use, they may be at a loss to know where questions should be emailed.

In addition, certificate authorities do not have a way to verify if the certificate is actually used as malware. But now, internet users can help the certificate authorities to identify malware – all internet users can send malicious files directly to the CCSS forum for examination and reporting.[2] After submission, CCSS will take over investigating and reporting the certificate to the appropriate authority. This allows consumers to be actively involved in the fight against malware.

Domain-validated certificates

The main problem with malware, to my mind, stems from the fact that malware sites can easily obtain Domain Validation (DV) digital certificates. DV certificates do not offer any assurances about the holder of the certificate. Instead, challenge-response email systems validate only the domain of the requester. If Joe at www.WeCheatGranny.com requests a domain-validated SSL certificate, no one at the certificate authority actually vets that application. The automated system issues the certificate, and www.WeCheatGranny.com is in business, ready to encrypt its communications without validating itself back to potential customers.

High-assurance digital certificates, on the other hand, offer internet users valuable information about the certificate holders. Organisation Validation (OV) and Extended Validation (EV) certificates are all vetted by human beings rather than machines. In the case of EV certificates, the certificate authority checks the legal existence of the holders. Fraudulent sites generally do not bother to register under such strenuous conditions.

"The rickety structure of the domain validation system means that everyone the public trusts to protect them on the internet must work together. If we don't, we will all fall apart and take the users with us"

An additional concern is that DV certificates are a potential venue for crackers to obtain DV certificates for sites they do not own, amplifying the threat of phishing and man-in-the-middle attacks. For example, at the 2008 Black Hat briefings, Mike Zusman disclosed that he had used an email challenge-response system to receive a signed certificate for a site that he did not own. Because this was handled by a simple automated check rather than by a person, he managed to issue a certificate for Login.live. com merely by creating an email alias for SSLcertificates@live.com.

The vulnerability Zusman discovered was that a DV certificate can often easily be issued to anyone with a tangential access to the domain name even if they don't have direct control over the domain or any affiliation with the domain. A spoofed certificate allows miscreants to siphon off the credibility of trusted sites. This abuses both internet users and honest website owners.

The rickety structure of the domain validation system means that everyone the public trusts to protect them on the internet must work together. If we don't, we will all fall apart and take the users with us.

The lack of minimum standards for security software

One problem with the security industry is that it lacks standards. It even lacks a good definition of what constitutes functioning security software.

A first step in improving security and mitigating the spread of rogue antivirus software is to figure out what actually constitutes security software and what is malware. Some so-called security software can even be malware in disguise. These fly-by-night scammers charge fees for security software but either do not install any protection or, even worse, install spyware. Fortunately, rogue antimalware software often has generally definable characteristics and installation methods that make detection easier.
Common characteristics include:

1. Aggressive 'scan and scare' functionality.
2. High rates of false positives.
3. Difficult or impossible removal systems unless the user makes a payment.

Because the characteristics are easy to spot, security vendors usually have little trouble eliminating out rogue or scareware products.

The second step in improving the quality of security software is that of defining what is a useful, working product and what is non-functional. The threats against which security software is designed to protect the user are changing. Challenges today include cross-site scripting such as PHP-include, buffer overflow attacks, and SQL injection (Figure 2).

No one wants security software that fights the last war. In light of changing hazards, standards for security software are hard to define. When the enemy keeps changing weapons and tactics it's hard to tell combatants how to protect themselves.

Assuming that there existed a standard for security software, there would still be the problem of trying to enforce it among developers, both in the US and outside. Additional questions that must be addressed to achieve this include:

1. Do we audit code?
2. Do we need signature- or behaviour based protection?
3. Do we need dynamic testing?
4. Do we perform leaktests?

These questions show how the understanding of certain terms of art differ between the security world and the consumers. Consumers, especially those with an interest in security, are becoming increasingly interested in leaktests, which are growing popular in security forums. However, leaktests, as currently performed, have limited value: they are merely shortcuts for true testing.

One question that plagues the industry includes questions about what actually constitutes useful leak information. For example, is a leaktest useful if it only tests a non-existent virus that might disable AV protection? Should leaktests only show that the purpose of the software can be bypassed?

Leaktests do not always emulate malware. But, because consumers are increasingly relying on the results, many vendors are adding unnecessary code and features to their software simply so they can meet leaktests. Failing to do so risks losing customers because of a meaningless lower rating.

"Leaktesting actually hurts consumers if it encourages poor design decisions in order to meet artificial tests"

There are lots of leaktests, but not all are useful. The tests can be broken down into high- and low-level tests. High-level tests change registry settings, send SSNs, etc. Low-level tests examine specific software functions. All good anti-malware software will probably pass the low-level tests.

High level leaktests are more problematic as they question how the software should respond to normal actions rather than how well the software protects against real malware. Many times this is a judgment call on the part of the software developer rather than a real security issue. For example, some leaktests require a block whenever a registry key changes. Whether or not this is done is really a design decision. Creating a message for each change leads to popup fatigue. Users stop paying attention, stop making good decisions, and turn off protection. Leaktesting actually hurts consumers if it encourages poor design decisions in order to meet artificial tests.

Generally, the user is the wrong person to ask for any question related to security. If security experts don't know the answer and can't answer it through their software, then the user won't know the answer and can't be expected to take the right action 100% of the time. No-one can afford to handicap the good guys by forcing the user to make decisions. Users don't have time to figure out the correct answers. In addition, because malware comes in a variety of formats and attacks, there is a need for many forms of security software. Declaring that one is significantly better than the other simply because it performs better in arbitrary leaktests is limiting protection rather than helping it.

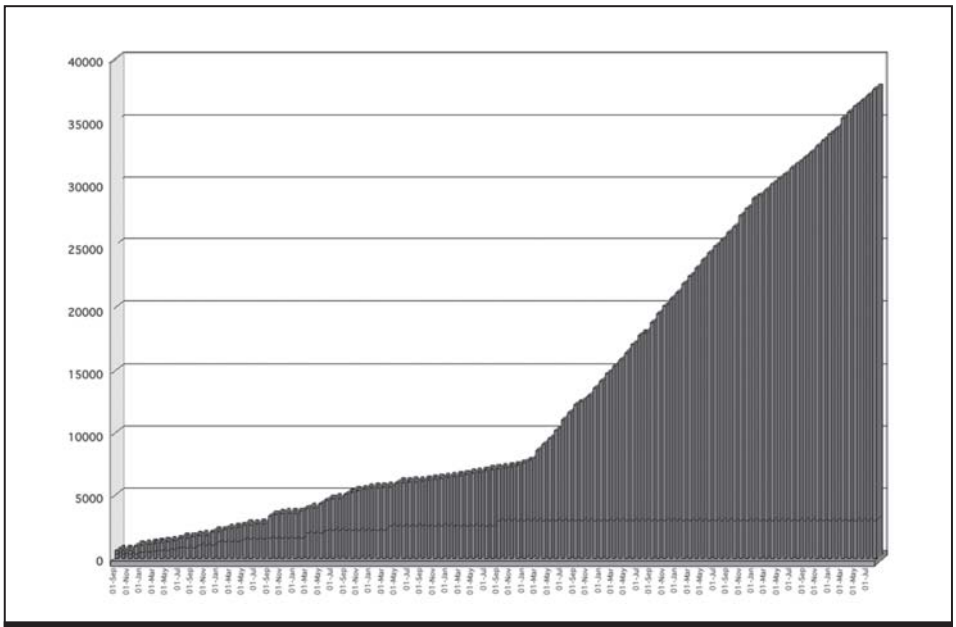

Figure 2: CVE Weakness Type Trends 2001-2007. Web-based vulnerabilities such as XSS and SQL injection have become much more popular, but buffer overflows continue to plague software. Courtesy: The MITRE Corporation.

Dynamic testing

This is why Comodo has joined the Anti-Malware Testing Standards organisation (AMTSO). AMTSO's dynamic testing promises to replace leaktests with more accurate dynamic testing. This will help eliminate the arbitrariness of leaktests and show how each security vendor does its own part in protecting consumers from real threats.

In the end, malware affects internet users everywhere. In order to be effective, we have to have a united front against malware that isn't limited to borders or specific pre-defined security classes. Enabling everyone to fight malware through activities such as the CCSS forum will help the world cut down on the malware infecting millions of computers.

All users, both security professionals and consumers, have a stake in maintaining the security of the internet. Everyone can play a part in keeping the internet safe. I encourage everyone to check out the Common Computing Security Standards Forum by visiting http://www.ccssforum.org and watching it closely for new and exciting ways in which everyone can participate in mitigating malware.

Further information

CVE Weakness Type Trends: http://cwe.mitre.org/documents/vuln-trends/index.html.

References

1. CCSS list of legitimate security software vendors: http://www.ccssforum.org/trusted-vendors.php

2. http://www.ccssforum.org/contact.Php

About the Author

Melih Abdulhayoglu, CEO and founder of Comodo, is an inventor, innovator and internet safety expert. He founded Comodo in 1998. Within the internet security industry, Abdulhayoglu works to promote higher standards. He founded the CA/B Forum, a consortium of Certificate Authorities and internet browser providers, which works together to provide higher authentication standards for digital certificates. He also began the Common Computing Security Standards Forum, allowing antivirus engines to work together with internet browsers to arrive at quality standards for protecting computer users. In 2008, Abdulhayoglu's efforts to promote internet safety, both through Comodo and within the industry, earned him Ernst & Young's Entrepreneur of the Year Award in the Information Technology Software category for New Jersey. He is a frequent speaker on internet safety issues. Abdulhayoglu earned a Bachelor of Science degree in Electronic Engineering from Bradford University in 1991.