May 2012

eset

Table of Contents

Antivirus, Antimalware, Flame and the RAT Factor

In terms of media coverage, one of the bigger malware stories in May was malicious code variously called The Flame, Flamer, or even Stryker (detected by ESET as Win32/Flamer.A). The story was a timely reminder that, from the earliest days of computer security there has been a gap between the knowledge and understanding of those who specialize in this field and those who are impacted by its failures and accomplishments. For example, the average computer virus expert, if such an animal could be said to exist, knows a whole lot more about viruses than the vast majority of people who become victims of viruses.

Unfortunately, this knowledge and awareness gap can become an obstacle to the adoption of computer security best practices if the potential victims do not grasp the full scope and extent of the threat that viruses present. At the same time the gap may impede communication between the public and the experts when new threats like Flame emerge. A rush to sensationalize a threat can be at odds with the fact that the threat is easily defeated by endpoint security and other security best practices. And that is why ESET has been working hard to expand consumer and corporate awareness of the nature of the malware threat today, seeking to close that gap, at least to the point where it ceases to impede the adoption of best practices.

Best Practices

Before talking further about the state of malware threats today, we should make clear the value of best practices, starting with their ability to prevent security problems. An organization that implements even the basic information security best practices has a much lower probability of suffering a costly security breach. Consider this finding from the Verizon Data Breach Investigation Report which analyzed 855 security incidents that occurred 2011, exposing 174 million records: 63 percent could have been prevented with measures categorized as “simple and cheap.” Another 31 percent could have been prevented with measures deemed “intermediate.” In other words, more than 9 out of 10 breaches would have been thwarted if organizations had followed best practices.

Best practices also have value if, despite best efforts, a breach does occur. The organization that can document its efforts to implement and adhere to best practices is in a much more defensible position with respect to claims of negligence by stakeholders and regulators, and better able to avoid adverse judgments in the courts of law, press, and public opinion.

The Malware Gap

While ESET researchers continue to dig deep into the technical details of complex malware threats such as Flame, Carberp, and Flashback, outside the labs and the inner circles of security experts it is still possible to meet people, even people attending information technology trade shows, who ask: “Does your antivirus product stop malware as well?” In other words, even an IT-aware subset of the general public is not universally up-to-speed with the adoption of malware—a contraction of malicious software—as an umbrella term for all computer viruses, worms, Trojans, backdoors, spyware, RATs, bots, and more (even as some malware experts cringe at the technically imprecise overlap of certain terms in that list).

Clearly, a lot of awareness raising needs to be done before all the potential victims of malware are fully cognizant of the security challenges they face. At the Interop trade show in Las Vegas this month, ESET devoted some of its resources to awareness raising by asking attendees, through several dozen live presentations, this question: “How serious can a malicious

software infection be these days?" Of course, the short answer is "Very serious indeed." Exactly how serious apparently came as news to many people according to feedback we received from the large number of attendees who watched the presentation.

In order to spread that news, ESET has now made the slides from that presentation available. In addition we have put together a 16 minute narrated video of the slide presentation called Package Delivery in a Flash. In that video people can see what a malware infection looks like to the bad guy who manages to get a RAT installed on a victim machine. That is R.A.T. for Remote Access Tool, one of the most popular categories of "crimeware" being deployed by cybercriminals today.

In the video we take a close look at one example—DarkComet RAT—the capabilities of which include stealing files and passwords from the victim machine and using the victim's webcam and microphone to spy on them, something that you might think was unique to Flame if you read some of the media coverage. In fact, this audio-visual spying capability was recently added to another piece of modular, point-and-click malware called SpyEye. (Note that ESET products detect SpyEye as Win32/Spy.SpyEye, Dark Comet RAT as Win32/Fynloski, and Flame as Win32/Flamer.A.)

The reality is that numerous pieces of malware offer similar abilities to Flame as well as modular design by which more features can be added. For example, one of the most prolific spam-sending botnets, Win32/Festi, is modular in design, as detailed at length in the recent ESET whitepaper on Festi. In terms of spying, DarkComet RAT is a good example of this genre of malware, which is probably one of the reasons it was chosen by the Syrian government when it needed a tool to conduct cyber espionage against its opponents, possibly as far back as May of last year, not long after the popular uprising began.

The ESET video on malware RATS also includes a description of the role that antivirus and endpoint security software can play in defeating this type of malware. Organizations that run antivirus on their file and email servers and their endpoints are well-protected, particularly if those endpoints have device controls in place.

In the video we point out that USB flash drives are being used as an attack vector when other avenues of malware delivery—like email file attachment and drive-by infection—are defeated by antivirus and website filtering/reputation tools. Fortunately, the USB threat can be thwarted with device and media controls installed on endpoints. The latest malware may come with lots of scary features, but you can drastically cut your chances of being on the receiving end of these attacks if you follow the best practice of deploying strong endpoint security software as part of your overall information security strategy.

Additions to the ESET Resources Pages

Papers/links recently added to the conference papers resources page at http://www.eset.com/us/resource/papers/conference-papers/:

- PIN Holes: Passcode Selection Strategies

By David Harley

Presented at the EICAR 2012 conference in May, this paper considers common strategies for selecting four-digit passcodes, and the implications for end-user security. Originally published in the EICAR 2012 Conference Proceedings. An earlier article for Virus Bulletin which was the starting point for this research

can be found here, by kind permission of Virus Bulletin: Hearing a PIN drop*

- After AMTSO: a funny thing happened on the way to the forum

By David Harley

Presented at the EICAR 2012 conference in May, this paper looks at how the Anti-Malware Testing Standards Organization might yet retain enough credibility to achieve its original aims. Originally published in the EICAR 2012 Conference Proceedings. The paper attracted the attention of Infosecurity Magazine, and the article that resulted can be read here: AMTSO has credibility gap for anti-virus testing standards. David blogged 'I continue to consider it essential for AMTSO – or an organization including or replacing it – to have better credibility than it does right now: if this initiative fails, testing is, in my eyes, close to useless because there will be no impartial authority to hold testers to account for the accuracy of their conclusions, and in the long run that will hurt their credibility.' And in an article for SC Magazine's Cybercrime Corner he wrote:

'Yesterday, I returned from the latest AMTSO workshop in Munich, where the membership discussed at considerable length how it could bridge its own credibility gap. And the favoured way of doing that seems to be by re-engineering the organization's internal structure in a way that looks more like a commercial enterprise (albeit run on a budget that at present would barely pay for a round of drinks at Google's Christmas party).

The likely form that will take is an executive team still consisting mostly of volunteers, but with the welcome addition of a paid administrator. In addition, the organization is considering returning to one of its early goals of monitoring and documenting ongoing testing, though probably in a less contentious form than its earlier review analysis process.

Whatever it takes, I guess. The question remains whether vendors and testers can play nicely enough together to keep the group alive. Even if they do, I'm not detecting a real sense that the organization needs to go far beyond cooperation between those two highly-partial groups and a highly specialized academic sector before it can claim to be establishing genuine standards. It needs to engage with a whole range of other stakeholders to get past the (un)popular perception of AMTSO as a vendor cartel. A more efficient business model should make it more effective in some senses. But will it also make it harder for people to remember AMTSO's non-profit status and intentions if it starts to look more like another hierarchical security company than a somewhat ramshackle aggregation of volunteers?'

- Man, Myth, Malware and Multi-Scanning

By David Harley & Julio Canto

The use and misuse of public multi-scanner web pages that check suspicious files for possible malicious content, and why they're no substitute for comparative testing.
Presented at the 5th Cybercrime Forensics Education & Training (CFET 2011) Conference in September 2011 .

Also added to the articles page containing articles written by or about ESET researchers at http://www.eset.com/us/resource/papers/articles/

- Living the Meme

By David Harley, February 2012

A comment piece on how apparently innocuous Facebook games might be used as part of a data aggregation attack.

Originally published in Virus Bulletin, February 2012*.

Added to the ESET presentations resources page at http://www.eset.com/us/resource/presentations/conferences/

- Carberp Evolution and BlackHole: Investigation Beyond the Event Horizon

By Aleksandr Matrosov, Eugene Rodionov, Dmitry Volkov and Vladimir Kropotov, May 2012

A joint presentation for the CARO workshop in Munich by researchers from ESET, Group-IB, and TNK-BP, summarizing their analysis of the technical features and criminal activity of Win32/Carberp and related malware.

See also the blog by Aleksandr Matrosov at http://blog.eset.com/2012/05/24/carberp-gang-evolution-at-caro-2012, and for some more leading-edge research on a very different example of malicious software, his earlier blog on King of Spam: Festi botnet analysis.

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 3
Percentage Detected: 6.36%

This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware that installs or modifies autorun.inf files as INF/Autorun unless it is identified as a member of a specific malware family.

Removable devices are useful and very popular: of course, malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default Autorun setting in Windows will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices: while this isn't always the program's primary distribution mechanism, malware authors are always ready to build in a little extra "value" by including an additional infection technique.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better, as Randy Abrams has suggested in our blog (http://blog.eset.com/?p=94 ; http://blog.eset.com/?p=828) to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case. You may find Randy's blog at http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun useful, too.

2. HTML/Iframe.B

Previous Ranking: 2
Percentage Detected: 4.84%

Type of infiltration: Virus

HTML/Iframe.B is generic detection of malicious IFRAME tags embedded in HTML pages, which redirect the browser to a specific URL location with malicious software.

3. HTML/ScrInject.B

Previous Ranking: 1
Percentage Detected: 4.09%

Generic detection of HTML web pages containing script obfuscated or iframe tags that that automatically redirect to the malware download.

4. Win32/Conficker

Previous Ranking: 5
Percentage Detected: 3.52%

The Win32/Conficker threat is a network worm originally propagated by exploiting a recent vulnerability in the Windows operating system. This vulnerability is present in the RPC sub-system and can be remotely exploited by an attacker without valid user credentials. Depending on the variant, it may also spread via unsecured shared folders and by removable media, making use of the Autorun facility enabled at present by default in Windows (though not in Windows 7).

Win32/Conficker loads a DLL through the svchost process. This threat contacts web servers with pre-computed domain names to download additional malicious components. Fuller descriptions of Conficker variants are available at http://www.eset.eu/buxus/generate_page.php?page_id=279&lng=en.

While ESET has effective detection for Conficker, it's important for end users to ensure that their systems are updated with the Microsoft patch, which has been available since the third quarter of 2008, so as to avoid other threats using the same vulnerability. Information on the vulnerability itself is available at http://www.microsoft.com/technet/security/Bulletin/ms08-067.mspx. While later variants dropped the code for infecting via Autorun, it can't hurt to disable it: this will reduce the impact of the many threats we detect as INF/Autorun. The Research team in San Diego has blogged extensively on Conficker issues: http://blog.eset.com/?cat=145

It's important to note that it's possible to avoid most Conficker infection risks generically, by practicing "safe hex": keep up-to-date with system patches, disable Autorun, and don't use unsecured shared folders. In view of all the publicity Conficker has received and its extensive use of a vulnerability that's been remediable for so many months, we'd expect Conficker infections to be in decline by now if people were taking these commonsense precautions. While the current ranking looks like a drop in Conficker prevalence, this figure is affected by the changes in naming and statistical measurement mentioned earlier: there's no indication of a significant drop in Conficker infections covering all variants.

5. JS/Iframe

Previous Ranking: 4
Percentage Detected: 2.85%

JS/Iframe.AS is a trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

6. Win32/Sirefef

Previous Ranking: 6
Percentage Detected: 2.66%

Win32/Sirefef.A is a trojan that redirects results of online search engines to web sites that contain adware.

7. Win32/Dorkbot

Previous Ranking: 9
Percentage Detected: 2.10%

Win32/Dorkbot.A is a worm that spreads via removable media. The worm contains a backdoor. It can be controlled remotely. The file is run-time compressed using UPX.
The worm collects login user names and passwords when the

user browses certain web sites. Then, it attempts to send gathered information to a remote machine. This kind of worm can be controlled remotely.

8. Win32/Sality

Previous Ranking: 12
Percentage Detected: 1.89%

Sality is a polymorphic file infector. When run starts a service and create/delete registry keys related with security activities in the system and to ensure the start of malicious process each reboot of operating system.
It modifies EXE and SCR files and disables services and process related to security solutions.
More information relating to a specific signature:
http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

9. JS/TrojanDownloader.Iframe.NKE

Previous Ranking: 7
Percentage Detected: 1.78%

It is a trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

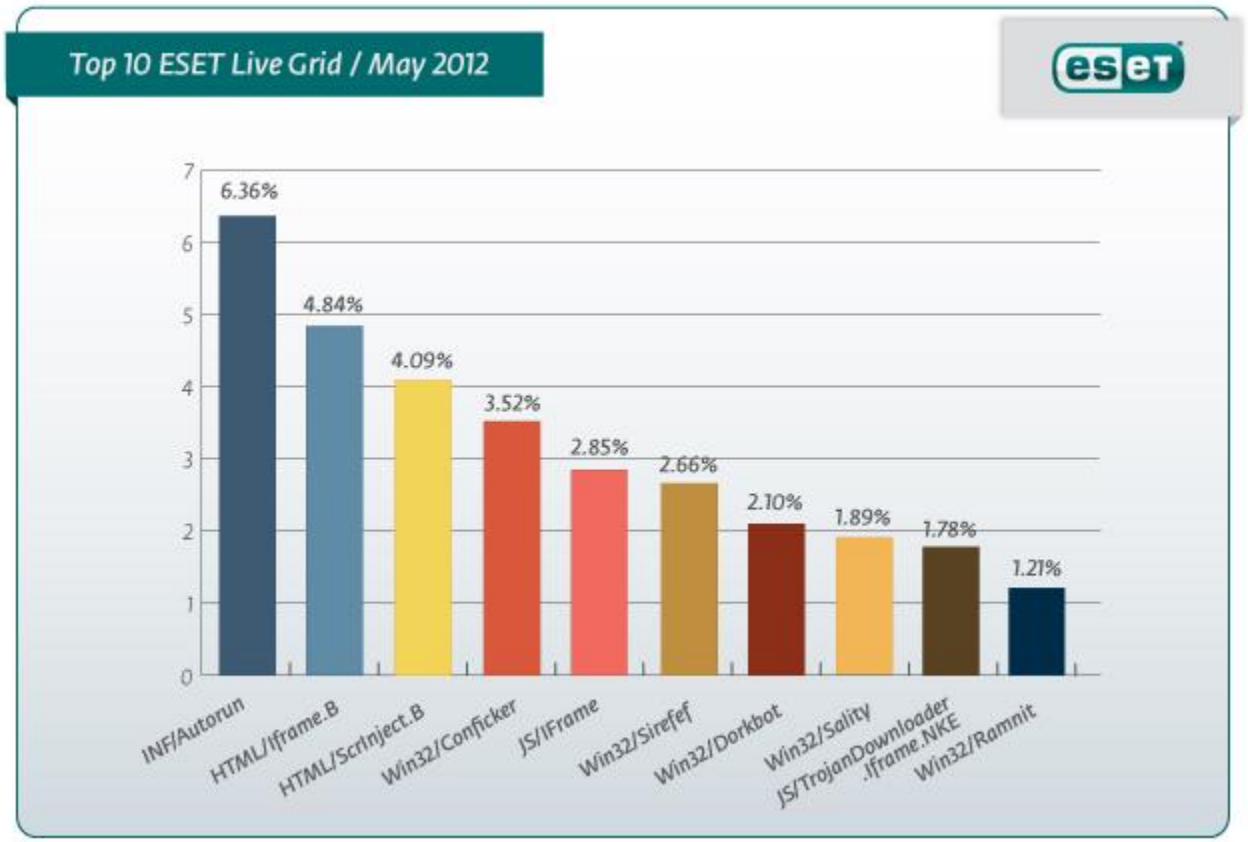
10. Win32/Ramnit

Previous Ranking: 13
Percentage Detected: 1.21%

It is a file infector. It's a virus that executes on every system start.It infects dll and exe files and also searches htm and html files to write malicious instruction in them. It exploits vulnerability on the system (CVE-2010-2568) that allows it to execute arbitrary code. It can be controlled remotley to capture screenshots, send gathered information, download files from a remote computer and/or the Internet, run executable files or shut down/restart the computer

Top Ten Threats at a Glance (graph)

Analysis of ESET Live Grid, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 6.36% of the total, was scored by the INF/Autorun class of threat.



About ESET

ESET is a global provider of security software. The ESET NOD32® Antivirus and ESET Smart Security products are consistently recognized among the most comprehensive and effective security solutions available today.

Additional resources

Keeping your knowledge up to date is as important as keeping your AV updated. For these and other suggested resources please visit the ESET Threat Center to view the latest:

- ESET White Papers
- ESET Blog
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation