NOTICEBORED

Spreading security awareness through social networks

Newsletter 155

2016 malware update

March 2016

Editorial

> “We are seeing just the beginnings of attacks and breaches against IoT devices”
>
> *McAfee*

What’s new in the world of malware? Bank Trojans and ransomware are hitting the news headlines more often than ever, while we’re seeing the emergence of sophisticated multifunctional malware and Malware as a Service (MaaS!). Criminals, terrorists and the intelligence services are actively investing in sneaky malware and clever malware-generating tools, while antivirus companies are getting ever richer. Where does that leave the rest of us? Struggling against the scourge of malware, doing the best we can.

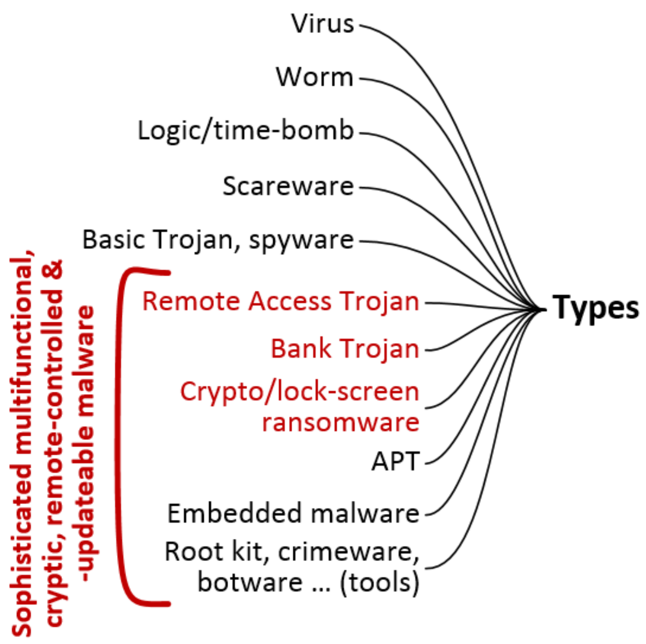
Awareness of malware is vital for employees, management and specialists. Alert workers should avoid risky situations (such as opening potentially infected email attachments or phalling for phishers), and will hopefully identify and report malware infections promptly. Managers need to appreciate the evolving malware risks in order invest appropriately in the controls and keep pace with developments in the field. IT and other professionals can help with the technical controls including, but going well beyond, antivirus software.

Gary Hinson, NoticeBored Editor

Introduction

“Computer viruses” have been around since the 1970’s when Creeper infected DEC PDP-10s and ANIMAL hit Univacs. While early infections were relatively trivial, mostly causing laughs or minor inconvenience, the Morris Worm in 1988 was an eye-opener for those labcoat-wearing data processing professionals of the day, revealing that networks could carry malicious traffic just as (in!)efficiently as the bits-n-bytes of research data.

We’ve come a long way since then, particularly in the last decade or so. We’ve been through the increasingly futile exercise of trying to name the individual types and families of malware, until now we are faced with hundreds of millions of new variants discovered every year including modular, obfuscated species almost impossible to characterize.


Virus
Worm
Logic/time-bomb
Scareware
Basic Trojan, spyware
Remote Access Trojan
Bank Trojan
Crypto/lock-screen ransomware
APT
Embedded malware
Root kit, crimeware, botware … (tools)
Types
Sophisticated multifunctional, cryptic, remote-controlled & -updateable malware

Malware-related risks

As usual, we'll break down the malware risks by briefly exploring the threats, vulnerabilities and impacts.

Malware threats

Who is responsible for creating and releasing malware? Good question! Naturally, they would prefer to stay in the shadows but we've managed to glean a few details. The main groups are:

1. VXers, hackers and crackers

'VXers' are the talented programmers doing the actual coding of malware, plus the associated tools used to sell, customize, deploy, maintain, update and control their babies in the field. As with hackers and definitely crackers, it's hard to resist the urge to label them criminals since they surely know that their products are mostly being used for criminal purposes, but some may conceivably be naïve or idealistic. Occasionally it is suggested that malware could roam the Internet, fixing the vulnerabilities it normally exploits … until the practicalities are taken into account, along with the possibility of legal action for making unauthorized changes, even if they were beneficial.

2. Unethical competitors, adversaries

Ethical competitors would surely never consider attacking the organization with malware … but that hinges on one's understanding of ethics. As in sport, commercial competition is so intense in some industries and situations that undoubtedly some players are more than willing to bend or break the rules to gain an advantage, especially if they believe they can get away with it. The covert nature of malware plays into their hands. The clever ones presumably work at arms-length through discreet advisors and agents, possibly even secretive government agencies as we'll see in a moment. Stealing trade secrets, grabbing lists of customers and prospects, sabotaging deals and deliberately harming a competitor's productivity or profitability are straightforward objectives that can be achieved through malware.

3. Criminals

Working alone, in gangs or in business-like enterprises ('organized crime'), criminals are making their fortunes through malware. It's much less stressful to buy or rent a Trojan than to don a ski mask and load a sawn-off shotgun to rob a bank! Organized criminals have the advantage of specialization and commercial services allowing them to buy or rent malware, exploit stolen information, launder the proceeds and remain under cover, although it must be a distinctly stressful existence to be dependent on crooks and surrounded by thugs.

4. Terrorists

Although there may be little evidence of direct terrorist involvement in malware, it would be surprising to learn that malware was *not* being used to raise funds, gather intelligence, conduct counter-intelligence and generally undermine or compromise their enemies. In dollar terms, the sheer global scale of malware is estimated to be on a par with the drugs trade, another nice little earner for terrorist groups, allegedly.

5. Governments & their agents

As with competitive organizations and athletes, *ethical* governments would presumably steer well clear of using malware to further their aims or protect their interests, but it's far from certain that governments generally are the least bit bothered about mere ethics. Perhaps I'm far too cynical and jaded but as I see things, malware is clearly just another tool for them, a class of cyberweapons if you will.

The involvement of secretive government agencies, secret agents/spies, the intelligence services, law enforcement, the militia and the broader defense industry gives a distinctly chilling edge to malware. They have *immense* resources and (to a large extent) immunity from prosecution. Last year we discussed APTs (Advanced Persistent Threats) as examples of the cutting-edge high-tech malware that are believed to originate with governments – the US and Israeli governments in the specific case of Stuxnet (we don't know for sure it was them but they have not convincingly denied their involvement).

6. Others

Forgive us if we get a bit vague when it comes to describing other parties or people that are involved with malware – they are hardly going to admit it openly. A few known examples are:

- Shady businesses advertising illicit wares through spam, thanks to the use of rented botnets;
- Parents and partners using spyware to keep a watchful eye on their loved ones;
- Malicious individuals with a grudge, or greedy or desperate enough to consider using malware. Occasionally for instance we hear about troubled IT pro's installing malware in their organizations' systems to 'compensate' them if they are dismissed.

Malware vulnerabilities

What is it that makes us vulnerable to malware?

1. Vulnerable software

Malware would be almost unheard-of if it were not for the litany of security issues in, say, Windows. You may think it unfair of us to pick on Bill Gates, and yet whereas he's no longer at the helm, his legacy is undeniably a massive global marketing machine turning out shoddy, insecure software that desperately requires patching on a depressingly frequent basis and yet never seems to get any better. To be honest, we could level much the same challenge against Android and even iOS: their popularity in the marketplace is probably the main determinant of the quantity and variety of malware, as opposed to their inherent design quality and security relative to Windows, although you might want to argue the point!

Application software security is a lottery!

Things are getting interesting in the mobile malware space too, and with IoT. A substantial proportion of mobile/portables are treated by their owners as intensely personal devices, who therefore rationalize their choice of dubious apps as lifestyle rather than business choices, even if they are provided by their employers for work purposes. IoT is presently in an even worse position, with miniscule hardware, minimal interfaces and largely missing support. Time to market and price are the primary drivers there, not security.

> Internet of things: IoT devices are just beginning to be exploited. The variety of devices, operating systems, and versions provides a near-term resistance to attack because few have a large enough installed base to attract cyber thieves. However, the sheer volume of devices has grown faster than we foresaw, and into industries that we did not expect, creating a massive attack surface—so it is only a matter of time until IoT device threats are widespread. Of course, attackers are not after the devices themselves, but the data or gateway capability that they enable. Attackers want the easiest way in and these devices often provide underdefended access to target-rich networks. We are seeing just the beginnings of attacks and breaches against them."
>
> *McAfee Quarterly Threat Report, August 2015*

2. Vulnerable hardware

Although it's unusual to think of security vulnerabilities in computer processors and the like, there's only so much that can be achieved in software. Just as malware exploits weaknesses in apps and operating system software, vulnerabilities in firmware, microcode and even hardware are certainly possible, and worth worrying about if you are facing extremely resourceful and determined adversaries. 'Embedded malware' was recently identified in Juniper firewalls, for example, installed before they left the factory: given their obvious network security rôle, the malware has led to a scramble among Juniper customers to deal with the incident.

Similar situations are *rumored* to have occurred with modems and mobiles produced for Western markets in the Far East, although the details are sketchy.

3. Vulnerable wetware

People are a significant cause of many malware incidents in the sense that we sometimes do silly things, fail to notice or ignore the warning signs, meddle with security settings, and generally pay scant attention to security (despite the *outstanding* awareness program!). As with hacking, social engineering is a complementary technique to purely technical attacks, convincing us to open emailed "invoices", "tickets" and "lottery wins", to install "games" and "utilities" (even "security software"!), to open "videos" or visit "news" sites – just a tiny selection of today's tricks of the trade.

> "Most of you know how important it is to have security software on your computers to stay protected from viruses, malware, spam and other Internet threats. Unfortunately, cybercriminals also know that it is critical to have security software, and they are using this knowledge to trick us into downloading fake antivirus software that is designed to do harm to your computer. Fake antivirus software is one of the most persistent threats on the Internet today. It masquerades as legitimate software, but is actually a malicious program that extorts money from you to "fix" your computer. And often, this new "antivirus" program disables your legitimate security software that you already have, making it challenging to remove."
>
> *McAfee blog, 2014*

Malware impacts

At a general level, malware can do anything that software can do, with tendency toward sneaky, underhand, mean-spirited, harmful and plan nasty things. Breaking it down a bit further:

- Business impacts include direct and indirect losses and costs, business disruption, loss of customers, reputation/brand damage and more. On top of that comes the not inconsiderable costs of malware controls – licenses for antivirus software just for starters. This awareness module could be covering something else if malware wasn't such a problem.
- Personal impacts include the loss of privacy caused by spyware, identify fraud leading to aggravation, if not losses, and the grief caused by permanently losing access to valuable information (such as irreplaceable family photos) encrypted by ransomware.
- Societal impacts include the cumulative expense of malware incidents and controls, the general loss of trust in IT, the effect on competitiveness and free markets, and the adverse consequences of malware funding organized crime and probably terrorism.

Forthcoming awareness topics

April – network security

Last month we discussed business relationships in 'supply networks', where multiple suppliers and intermediaries supply goods and services to multiple customers. Next month we'll be exploring the information risk and security aspects of ICT networks linking multiple organizations and people in a complex mesh.

May – industrial information security

May's module brings together the information security aspects of SCADA/ICS (microcontrollers embedded in industrial machinery, plant, buildings and vehicles) and cybersecurity in the specific sense of protecting critical infrastructures for the good of society.

June – trust and ethics

We take a lot of things 'on trust', believing that they will go to plan and work in our favor. Life would be extremely difficult otherwise, so are we force to just go with the flow, or are there things we can do to stack the odds our way? ■