Security awareness – management brief

Malware

NOTICEBORED

March 2016

Executive summary

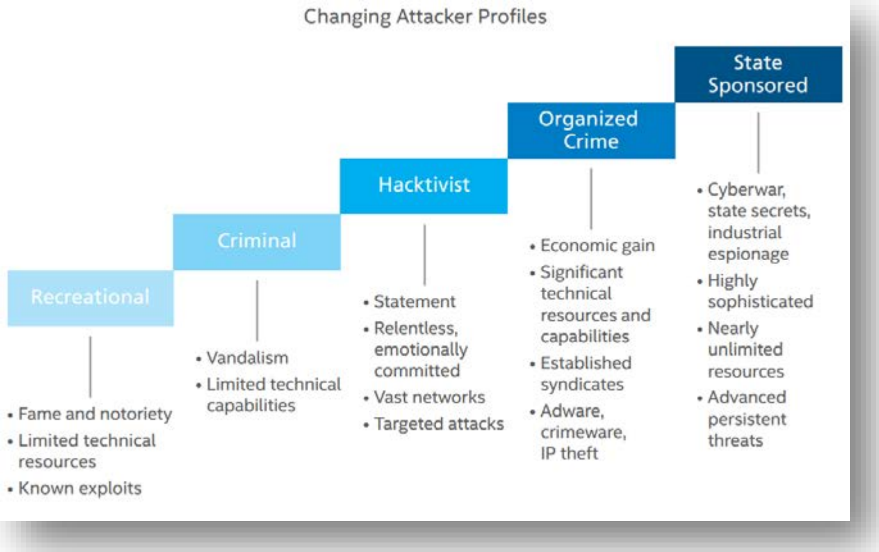
Malware (malicious software) is a significant risk for all organizations that depend on information systems themselves, or on other IT-dependent organizations. There are indications that malware risks are escalating while security controls are losing pace, hence it is increasingly necessary to plan and prepare for serious malware incidents to ensure business continuity.

Security awareness brief

Malware

Introduction

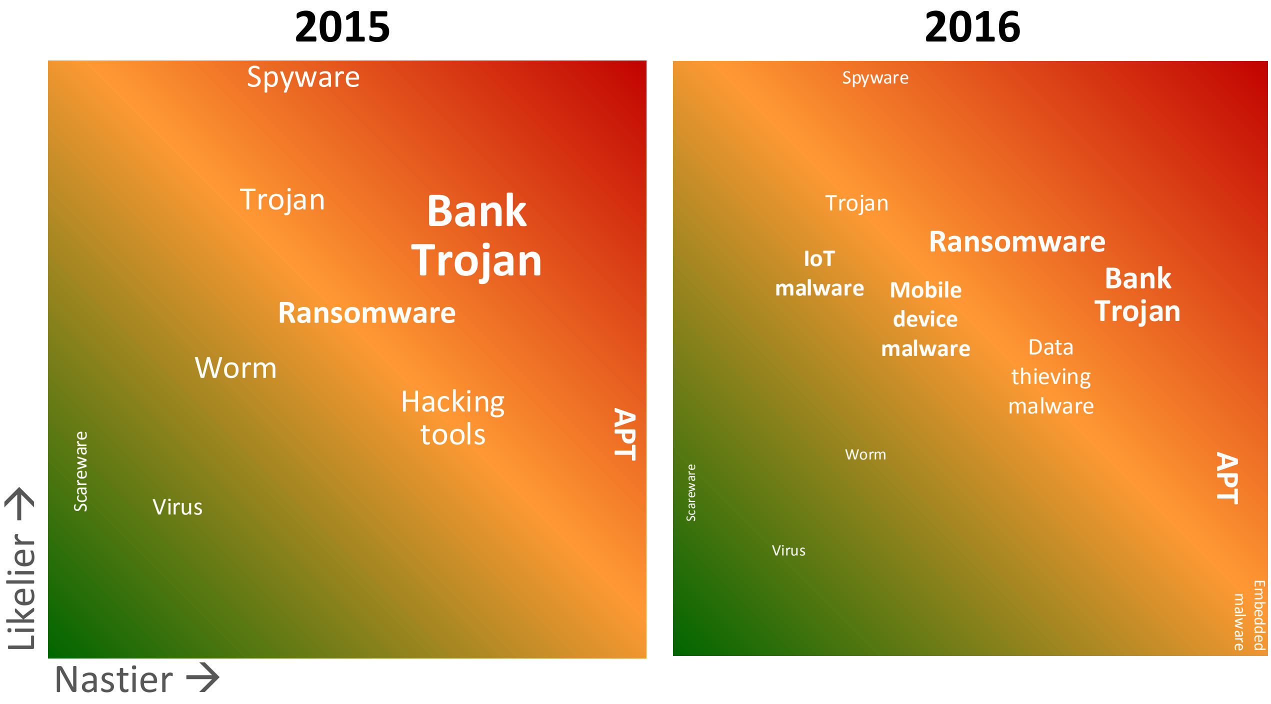
Since the 1970s, **mal**icious soft**ware** including computer viruses, network worms, Trojan horse programs and other nasties have been causing problems for computer users. The threat level has steadily escalated throughout the period. Antivirus company McAfee outlined the evolution of malware in their August 2015 Quarterly Threats Report –>


Changing Attacker Profiles
Recreational
• Fame and notoriety
• Limited technical resources
• Known exploits
Criminal
• Vandalism
• Limited technical capabilities
Hacktivist
• Statement
• Relentless, emotionally committed
• Vast networks
• Targeted attacks
Organized Crime
• Economic gain
• Significant technical resources and capabilities
• Established syndicates
• Adware, crimeware, IP theft
State Sponsored
• Cyberwar, state secrets, industrial espionage
• Highly sophisticated
• Nearly unlimited resources
• Advanced persistent threats

Today's threats are mostly criminals intent on stealing personal identities, credit card numbers and valuable intellectual property, draining corporate bank accounts, or extorting money from victims by holding their systems and data to ransom.

It appears that governments are also using malware as cyber-weapons to compromise other nations for military and/or political ends, including industrial or economic espionage and sabotage ('cybertage').

We've noticed changes in the malware risk picture during the past year:



We identified bank Trojans as a concern last year: these are programs targeting (mostly) Finance Department professionals with online access to corporate bank accounts. While everything *appears* normal on the screen, the criminals are stealing funds by submitting fraudulent transactions in the background. The incidents typically involve social engineering methods such as phishing and infected email attachments, perhaps fooling unaware accounts clerks into opening fake invoices.

Ransomware was also picked out as a significant risk following the Sony hack at the end of 2014. In that case, malware was used to steal unreleased films and other valuable intellectual property from Sony's internal network. Presumably after making their ransom demands, the scammers upped the ante by disclosing commercial sensitive and highly embarrassing emails, while destroying Sony's IT systems, causing immense business disruption. Many other ransomware attacks are occurring although it appears that most victims are either quietly paying the ransoms (usually just a few hundred dollars, it seems) or rebuilding their systems from backups and belatedly improving security to lock the scammers out, hopefully keeping themselves out of the news headlines. A recent widely-publicized incident involved a demand for $17,000 from a private hospital in Los Angeles: the hospital caved-in to the demand to obtain the key needed to decrypt their systems and restore business operations, although as with kidnapping there is no guarantee that the criminals will deliver on their promises once the ransom is paid. Worse still, the victim organizations who accede to the demands are admitting their vulnerability, perhaps marking themselves out for further attacks unless they are somehow able to boost their cybersecurity in a hurry.

Emerging malware risks

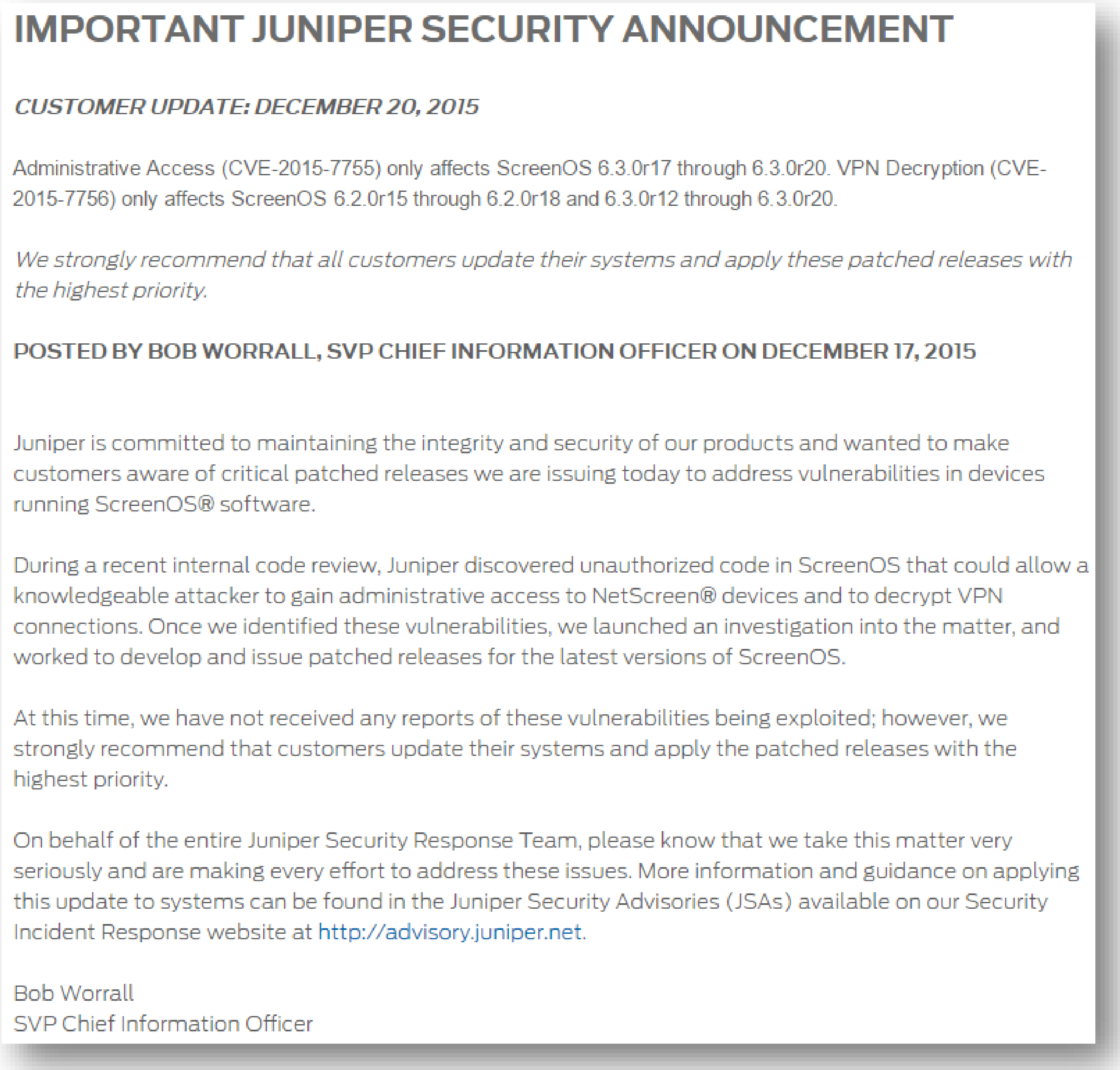
Four new or increasing risks shown on the 2016 risk diagram above are particularly worth noting:

IoT malware is malware infecting Internet of Things devices such as home and office automation systems, electronic door locks and Internet-enabled refrigerators. IoT is a rapidly-expanding market with immense pressure on suppliers to release sexy new products before competitors, and at lower prices. Security standards are lagging way behind product developments. The first-wave diminutive devices are often technically constrained and hence incapable of running antivirus software or other security controls, while naïve customers typically don't even consider the cybersecurity angle until, maybe, it's too late. As IoT devices spread, we may be inadvertently installing a giant distributed network of insecure IT systems ripe for exploitation by hackers, scammers, fraudsters, snoops and spooks.

Mobile device malware targets mobile/portable IoT devices and conventional systems such as laptops, tablet PCs and smartphones. Modern malware is also becoming more mobile in that it is able to infect a wide range of systems – not just Windows but Linux, iOS and MacOs, for instance. Criminals and hackers are making money by using or renting out networks containing hundreds or thousands of compromised systems ('botnets') for various nefarious purposes … and reinvesting some of the income to create ever more sophisticated malware (more on that below).

Data thieving malware is designed to extract valuable information surreptitiously from corporate networks and individual systems including home office desktops, laptops and so on plus point-of-sale retail systems and ATMs (Automated Teller Machines). Stolen personal information, payment card numbers *etc.* may be used for identity theft or extortion, while stolen intellectual property and trade secrets may be exploited directly or sold to unethical competitors to gain an unfair commercial advantage (economic espionage).

Embedded malware in the extreme bottom right corner of the 2016 risk graphic is presently little more than a theoretical risk of concern to government spooks and the military … but aside from rumors, at least one definite embedded malware incident has hit the news already. Juniper firewalls were discovered to have been pre-infected with malware before they even left the factory. Firewalls, of course, are used to protect sensitive networks, systems and data, hence there are troubling implications since it appears some malicious actor was able to decrypt and read confidential network traffic that the firewalls were *supposed* to keep secure:



IMPORTANT JUNIPER SECURITY ANNOUNCEMENT

CUSTOMER UPDATE: DECEMBER 20, 2015

Administrative Access (CVE-2015-7755) only affects ScreenOS 6.3.0r17 through 6.3.0r20. VPN Decryption (CVE-2015-7756) only affects ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20.

We strongly recommend that all customers update their systems and apply these patched releases with the highest priority.

POSTED BY BOB WORRALL, SVP CHIEF INFORMATION OFFICER ON DECEMBER 17, 2015

Juniper is committed to maintaining the integrity and security of our products and wanted to make customers aware of critical patched releases we are issuing today to address vulnerabilities in devices running ScreenOS® software.

During a recent internal code review, Juniper discovered unauthorized code in ScreenOS that could allow a knowledgeable attacker to gain administrative access to NetScreen® devices and to decrypt VPN connections. Once we identified these vulnerabilities, we launched an investigation into the matter, and worked to develop and issue patched releases for the latest versions of ScreenOS.

At this time, we have not received any reports of these vulnerabilities being exploited; however, we strongly recommend that customers update their systems and apply the patched releases with the highest priority.

On behalf of the entire Juniper Security Response Team, please know that we take this matter very seriously and are making every effort to address these issues. More information and guidance on applying this update to systems can be found in the Juniper Security Advisories (JSAs) available on our Security Incident Response website at http://advisory.juniper.net.

Bob Worrall
SVP Chief Information Officer

Source: Juniper customer announcement, 20th December 2015

Malware could potentially be embedded in many other systems, possibly buried deep within the computer processor chips and memory, disk, video, network or keyboard controllers. The microcode or firmware controlling their internal operations has low-level access and capabilities that could remain completely hidden from higher-level operating systems and application programs, including antivirus software. However, the extreme technical skills and access needed to develop and deploy such malware and install and exploit it without being detected suggest that the threat is likely to be mostly military rather than criminal in nature, making this a risk of concern to governments, militia, the defense industry and critical national infrastructure organizations but less likely to impact the rest of us directly – as far as we know, anyway, but that could change.

What's looming over the horizon?

"**Advanced Persistent Threat**: a highly sophisticated, sustained and damaging series of attacks by a particularly resourceful, determined and capable adversary." *Wikipedia*

Those four emerging risks, plus APTs (Advanced Persistent Threats), bank Trojans and ransomware, share advanced technical capabilities hinting at what we might expect from the *next* wave of malware. Specifically, modern malware is:

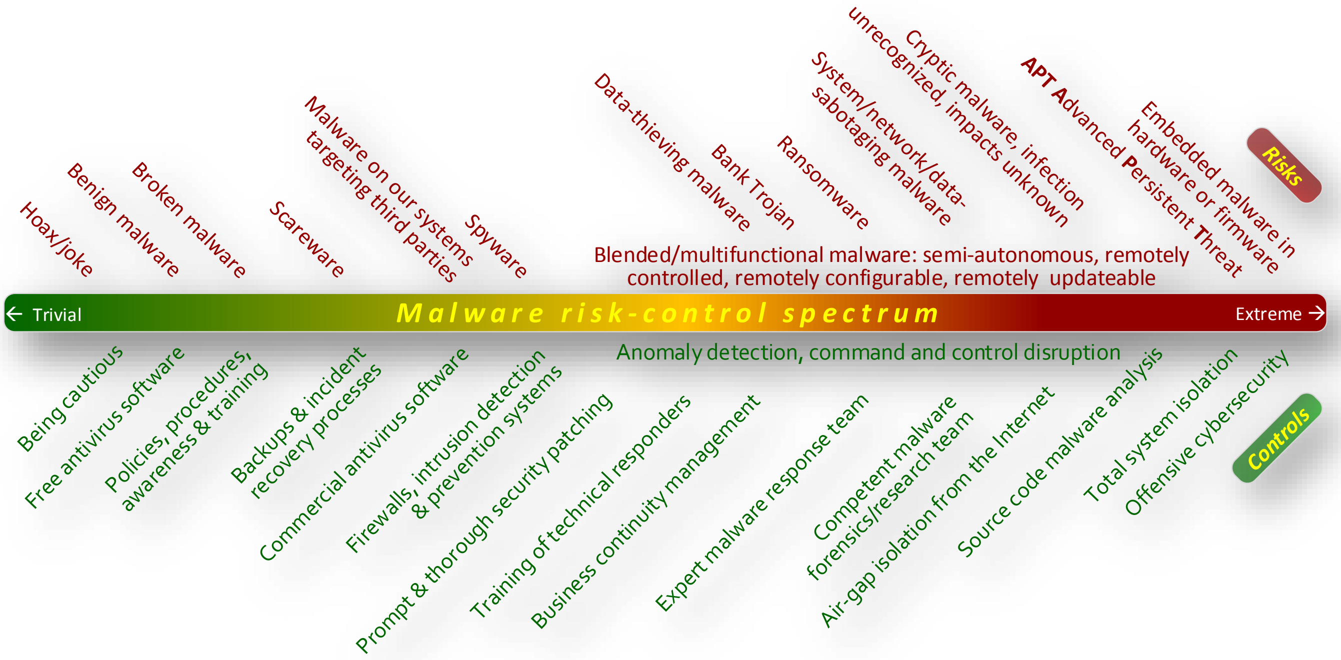
- **Multifunctional** combining worms and Trojans with social engineering and other capabilities, including an ever-expanding range of payloads to exploit a wide variety of vulnerabilities;
- **Remotely-controlled** allowing criminals or military units to communicate with their malware agents in the field, as it were, issuing new commands and retrieving stolen information;
- **Semi-autonomous** meaning that to some extent it can 'look after itself' and pursue various objectives (*e.g.* gathering intelligence) while not actually being remotely-controlled by its human masters;
- **Modular and remotely reconfigurable** for instance allowing hackers to install functions that exploit newly-identified technical vulnerabilities (so-called zero-days), to attack additional targets (*e.g*. infecting those accounting professionals mentioned earlier having initially entered the corporation's systems through a random employee's inattentiveness or a network security weakness);
- **Highly variable** through widespread use of encryption, such that simple pattern-matching on the underlying code is no longer adequate to identify today's malware, and skilled forensic analysts find it difficult to determine precisely what the malware is up to;
- **Extremely stealthy,** able to remain undetected and hence unchallenged for long periods of time, perhaps *years* at a stretch. We're looking for camouflaged needles in haystacks.

In risk terms, the malware threat is increasing, taking advantage of an expanding vista of vulnerabilities, and causing material impacts on individuals, organizations and the wider society. Taken as a whole, the malware risk looks set not just to remain a problem for the foreseeable future, but to get worse.

"Strange as it may sound, the computer virus is something of an Information Age marvel. On one hand, viruses show us how vulnerable we are - a properly engineered virus can have a devastating effect, disrupting productivity and doing billions of dollars in damages. On the other hand, they show us how sophisticated and interconnected human beings have become." *How Stuff Works*

Malware controls

The spectrum diagram illustrates the wide range of malware risks and controls:


Hoax/joke
Benign malware
Broken malware
Scareware
Malware on our systems targeting third parties
Spyware
Data-thieving malware
Bank Trojan
Ransomware
System/network/data-sabotaging malware
Cryptic malware, infection unrecognized, impacts unknown
APT Advanced Persistent Threat
Embedded malware in hardware or firmware
Risks
Blended/multifunctional malware: semi-autonomous, remotely controlled, remotely configurable, remotely updateable
← Trivial
Malware risk-control spectrum
Extreme →
Anomaly detection, command and control disruption
Being cautious
Free antivirus software
Policies, procedures, awareness & training
Backups & incident recovery processes
Commercial antivirus software
Firewalls, intrusion detection & prevention systems
Prompt & thorough security patching
Training of technical responders
Business continuity management
Expert malware response team
Competent malware forensics/research team
Air-gap isolation from the Internet
Source code malware analysis
Total system isolation
Offensive cybersecurity
Controls

New, even more sophisticated and capable malware-based cyberweapons are constantly being researched, developed and deployed for both military and criminal purposes, placing current security controls under immense pressure. Antivirus software, firewalls, intrusion detection and prevention systems, and prompt security patching are necessary controls, along with backups, policies and awareness activities such as this briefing, all of which are towards the low end of the spectrum.

Controls in the middle ground include better incident response and sophisticated forensics capabilities to detect and tackle advanced malware. 'Anomaly detection' is a technique for spotting possible malware, hacking or other incidents due to unusual patterns or levels of activity – tricky to achieve in practice because it revolves around differentiating suspicious from normal changes on flimsy evidence. 'Command and control disruption' is being used by the authorities and antivirus companies to clamp down on the remote control aspects noted earlier, along with traditional crime-fighting methods to frustrate criminal organizations, money laundering and profiteering.

Up at the extreme end of the scale, the security controls are beyond the means of all but a few well-resourced organizations, mostly military or governmental. Analyzing source code for microcode, firmware, operating system and application software, and examining the technical design of microprocessors and device controllers is something that has previously been almost entirely down to the IT equipment manufacturers, but maybe that too will change.

Conclusion

Given the choice, completely avoiding malware risks by not using IT would be a valid option but it is practically impossible these days to eliminate computer systems and networks and still remain in business.

A less effective though still valuable approach is to educate motivate workers to spot, report and/or avoid the more obvious malware risks such as phishing attacks, suspicious email attachments, computer storage media and devices, hence the need for malware policies, awareness, training and compliance activities. Vigilance is a relatively cheap control.

Conventional malware controls such as good antivirus software, prompt system patching and backups still earn their keep, while incident detection and response processes, perhaps coupled with anomaly and intrusion detection systems and forensic capabilities are increasingly important as malware grows ever more sophisticated and stealthy.

Business continuity including resilience, recovery and contingency arrangements, and possibly insurance, provide back-stops to limit the impact of serious malware or other information security incidents, including those affecting business partners, the supply chain, the industry or conceivably the nation and global economy.

For more information

Browse the intranet *Security Zone*, call the Help Desk or contact Information Security.