NOTICEBORED

Malware update 2016

Abstract

Find out what has changed
in the world of malware
during the past year,
and what worries us now

Security awareness brief

Professionals

March 2016

Important note

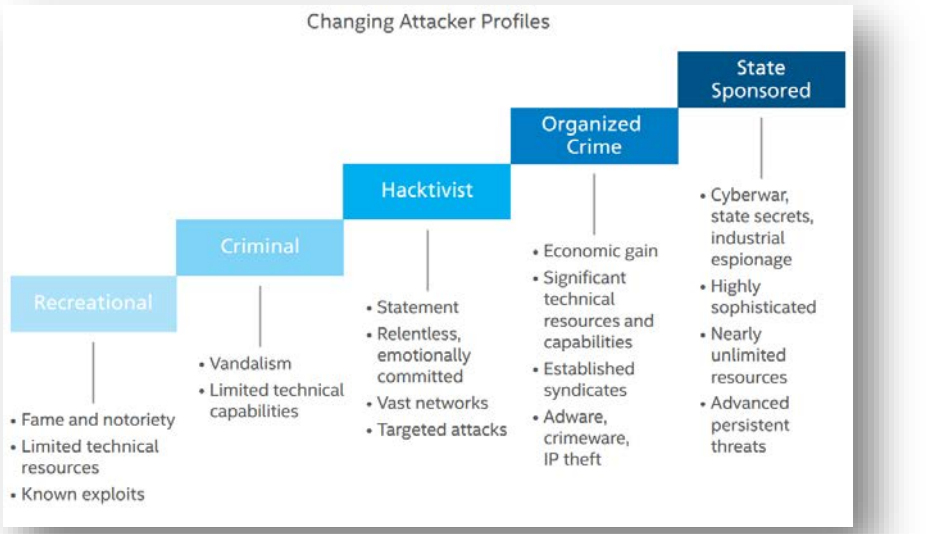
The *generic* advice in this briefing may not suit a given organization

Professionals' security awareness briefing

Malware

Introduction

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



Initially, malware was a bit of a joke – literally – with jolly japes such as viruses that swapped the character set to make users think their terminals had been turned upside down.

Today malware is no laughing matter. Malware is used by organized criminals to steal personal identities, credit card numbers and valuable intellectual property, drain corporate bank accounts, or extort money by holding systems and data to ransom. They have the social networks, tools and capabilities to buy or rent customized malware and lists of potential victims, as well as the money laundering and other 'support services' to profit from their ill-gotten gains without (usually) being caught.

Worse still, governments are also using malware as cyber-weapons to compromise other nations for military and/or political ends, including industrial or economic espionage. Whereas criminals can and do invest in their tools, governments have the advantage of deeper pockets, legal and (arguably) moral justifications, and access to highly skilled malware analysts and authors ('VXers').

Malware evolution

In the beginning came BRAIN.A, the first *personal computer* virus created in 1986 as a proof-of-concept by two Pakistani geeks who subsequently set up an ISP called Brain Communications. Strictly speaking, BRAIN.A should not have been called a virus since it did not attach itself to executable programs, but that's incidental. It was spread on floppy disks (remember them?) and spread it did, infecting a substantial proportion of the clunky steam-powered computers used by keen computer hobbyists and data processing professionals of the day. Other early viruses included Creeper (DEC PDP-10, 1971), ANIMAL/PERVADE (Univac, 1974) and Elk Cloner (Apple II, 1981).

Next came worms that spread via networks, including of course the Internet. The Internet Worm (1988) was written and released by Robert Tappan Morris as an 'experiment' to determine the size

of the Internet. An unfortunate side-effect was that many systems failed, making it easier to count the remainder I guess.

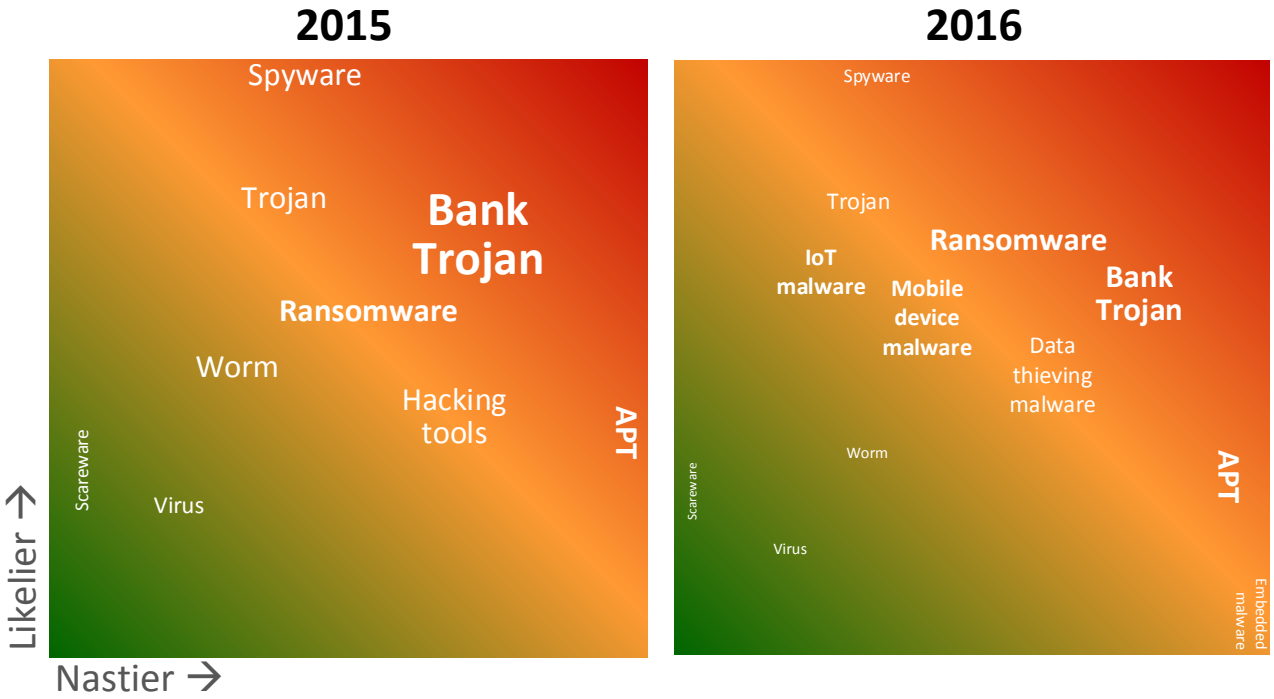
In the 1990s we saw the rise of antivirus software, first as a mechanism to halt the spread of malware and soon as a method to make money. The arms race between VXers and antivirus companies has continued ever since, both sides profiting from their respective skills.

In the 2000s, Trojans started causing grief by spying on computer users, secretly capturing their key-presses to steal passwords and credit card numbers. The banks are still battling the Trojan scourge, now grown much more sophisticated and sneaky in order to negate various controls introduced by the banks in an attempt to stem their losses.

During the past decade or so, we've seen the meteoric rise of portable computing, WiFi and mobile networks plus always-on high-speed broadband, along with the whole social media/social networking phenomenon. Modern smartphones, marvels of miniaturization, have taken over where analog cellphones with batteries the size of bricks, Personal Digital Assistants, and diaries left off … and along with laptops and tablets, they have become the battleground for mobile malware.

Evolving malware risks

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



As you'll see from last year's Analog Risk Assessment (ARA) graphic, we were worries about **bank Trojans** targeting (mostly) Finance Department professionals with online access to corporate bank accounts. While everything *appears* normal on the screen, those naughty criminals are stealing funds by submitting fraudulent transactions and diverting funds in the background. Infections may involve social engineering methods such as phishing and infected email attachments, perhaps fooling unaware accounts clerks into opening fake invoices. Laundering the money is very slick, thanks again to the use of IT including money mules and Bitcoin.

Ransomware was also picked out in 2015 as a significant risk following the Sony hack at the end of the previous year. 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 (we're still not entirely clear about the details, such as whether the North Koreans were or were not behind the attack), 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

As you'll see from the 2016 ARA graphic, four new or increasing risks give us cause for concern this year.

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 are in effect installing a giant distributed network of insecure IT systems ripe for exploitation by hackers, scammers, fraudsters, snoops and spooks.

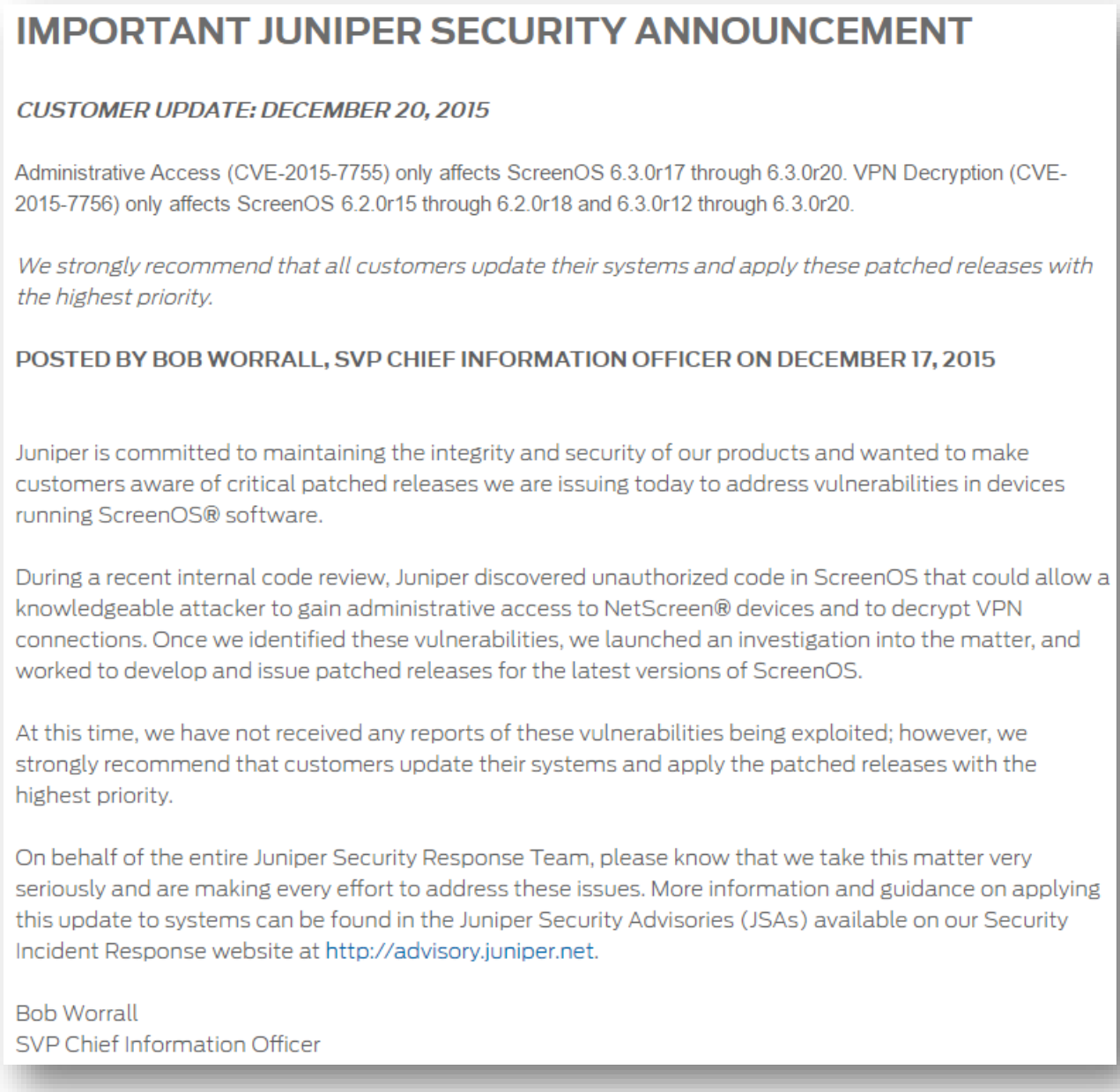
Years ago, people used to say "I'm really not bothered about viruses on my computer – there's nothing of interest on there anyway". Spyware put a slightly different edge on the risk but the blasé attitude persists, through to *things* that their owners find trivial, so not worth securing. The trouble is they are providing network platforms on which malware can establish beachheads from which to broaden and deepen their attacks – for instance participating in DDoS (Distributed Denial of Service) attacks or sending spam, and snooping on local network traffic for other exploitable opportunities.

Mobile device malware targets both mobile/portable IoT devices and more conventional systems such as laptops, tablet PCs and smartphones. Modern malware is able to infect a wide range of operating systems – not just Windows but Linux, iOS and MacOs too. Some malware is written in Java specifically to work across platforms (mobile mobile malware!). 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 PoS (Point-of-Sale) retail systems and bank 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, used for coercion (threatening disclosure or destruction) 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?

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:

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

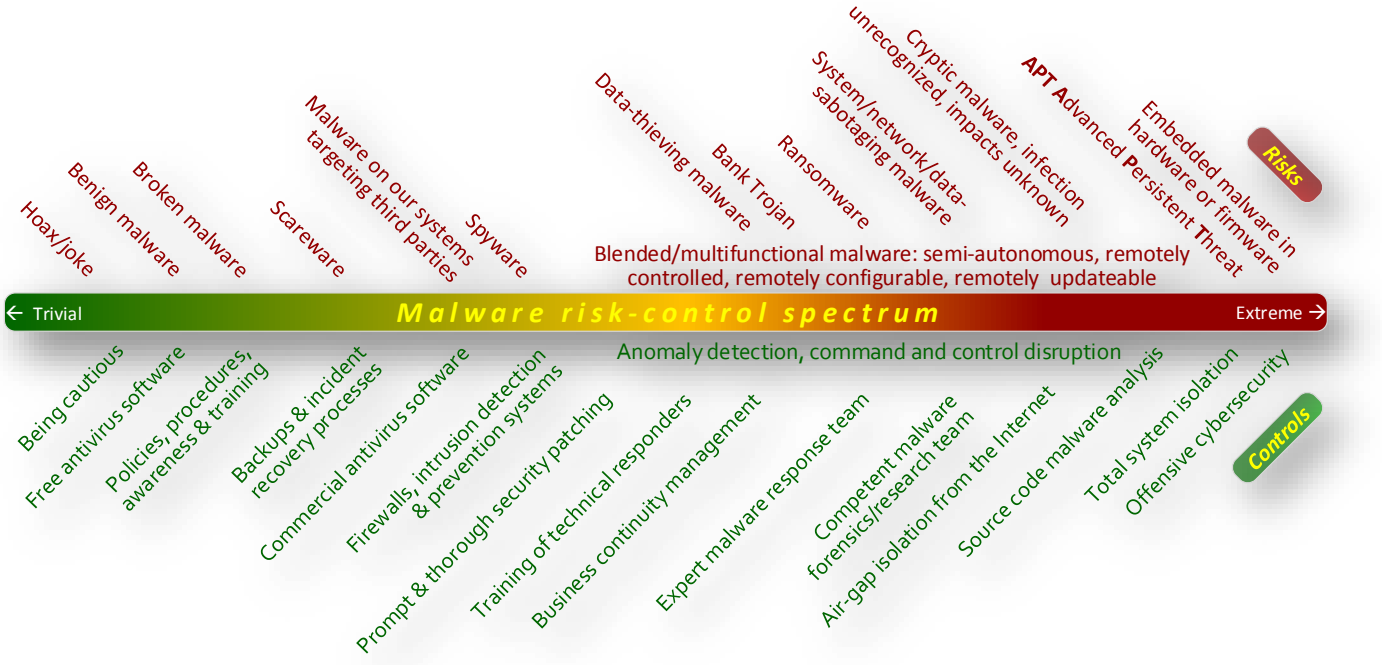
- **Multifunctional** combining worms and Trojans with social engineering and other capabilities, including an ever-expanding range of payloads to exploit a wide variety of vulnerabilities;
- **Remotely-controlled** allowing criminals or military units to communicate with their malware agents in the 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:



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. Such basic controls are necessary but not sufficient to address the growth of more sophisticated malware.

Controls in the middle ground include strong incident response processes and sophisticated forensics capabilities to detect and tackle advanced malware. Anomaly detection attempts to detect malware activity due to unusual patterns – tricky to achieve in practice because it revolves around differentiating suspicious from normal changes on flimsy evidence, but with the added bonus of perhaps identifying hackers, bandwidth hogs, errant systems and software, and other issues (such as network devices unexpectedly spewing out reams of DNS queries or VOIP traffic).

Command and Control (C^2) 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. Taking down the C^2 networks and systems takes away the criminals' ability to communicate with their bots. The VXers don't make it easy for the authorities, though, using various schemes to obfuscate and dynamically update the networks, for example using round-robin and redirection. In one case, *someone* with a sense of humor changed the C^2 server to broadcast a message back to the owners of infected computers when the malware 'phoned home', warning them about their infection.

Up at the extreme end of the risk spectrum, 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 *etc.* for malicious or suspicious code 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 might be a valid option for the organization but *DON'T PANIC*! We all know it is practically impossible these days to eliminate computer systems and networks and still remain in business. This is not a viable choice.

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. We're counting on professionals like you to help us here, not least by being hyper-sensitive towards the malware threat – especially if you have privileged accounts and access to the corporation's crown jewels.

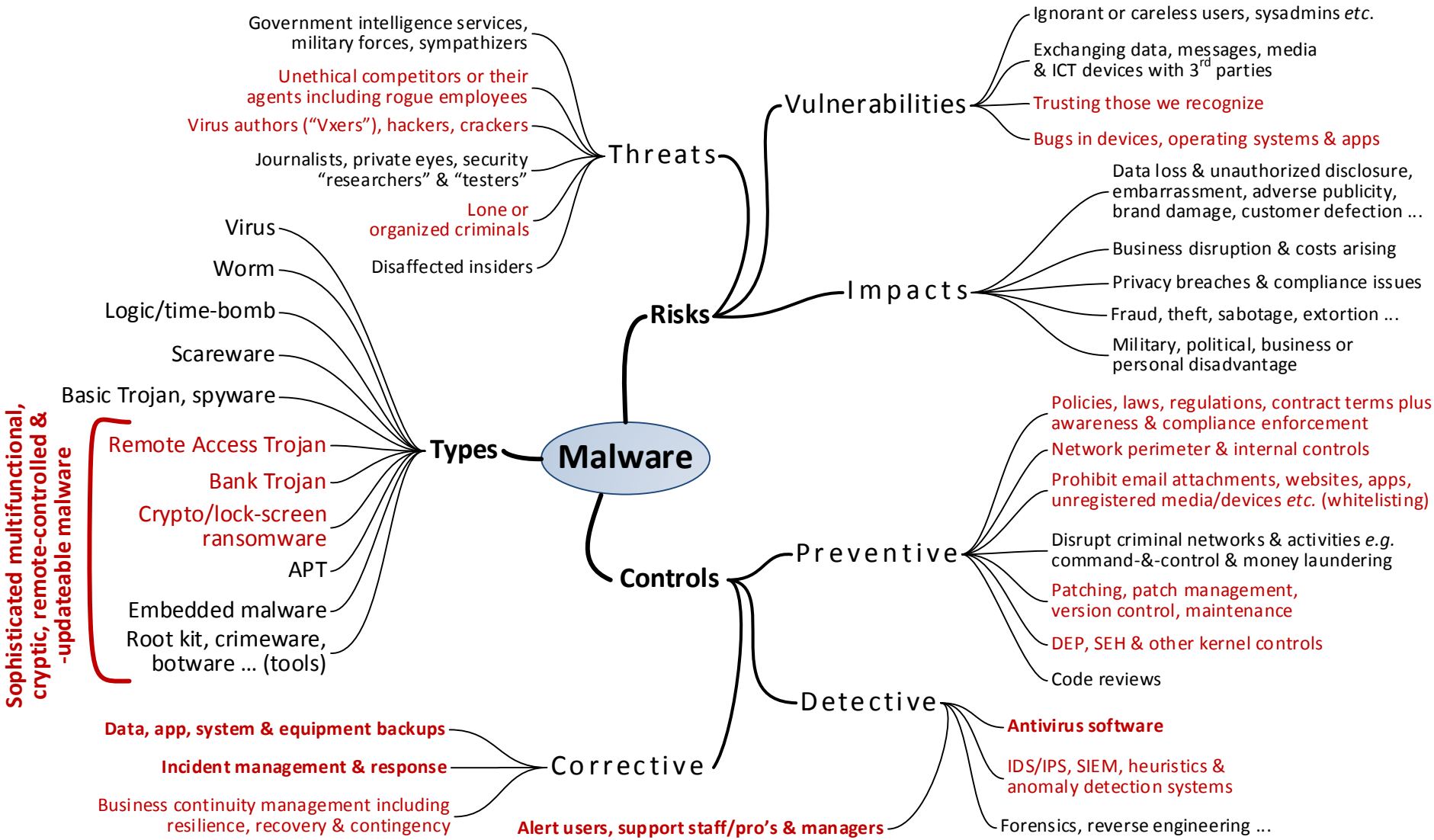
Conventional malware controls such as antivirus software, prompt system patching and backups still earn their keep, while incident detection and response processes, perhaps coupled with anomaly and intrusion detection systems and forensic capabilities are increasingly important as malware grows ever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

Business continuity including resilience and disaster recovery arrangements, and possibly insurance, are 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. You may argue that we suffer more than enough malware incidents to ensure that the incident management processes are well exercised, but we also need to be ready to respond effectively to those once-in-a-blue-moon crazy malware outbreaks - the Warhol worms, concerted cyberattacks, bank Trojans and ransomware on steroids … and there's always the "something else has gone horribly wrong" contingency situation to bear in mind.

For more information

Visit the intranet *Security Zone*, call the Help Desk or contact Information Security about malware.

PS For those of you who prefer pretty pictures to prose, the mind-map overleaf summarizes this briefing. In our considered opinion, the things picked out in red are more important than most, while those in **bold red** are critical … but feel free to disagree, and chat about it with your colleagues.


Malware
Risks
Threats
Government intelligence services, military forces, sympathizers
Unethical competitors or their agents including rogue employees
Virus authors ("Vxers"), hackers, crackers
Journalists, private eyes, security "researchers" & "testers"
Lone or organized criminals
Disaffected insiders
Vulnerabilities
Ignorant or careless users, sysadmins etc.
Exchanging data, messages, media & ICT devices with 3rd parties
Trusting those we recognize
Bugs in devices, operating systems & apps
Impacts
Data loss & unauthorized disclosure, embarrassment, adverse publicity, brand damage, customer defection ...
Business disruption & costs arising
Privacy breaches & compliance issues
Fraud, theft, sabotage, extortion ...
Military, political, business or personal disadvantage
Types
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)
Sophisticated multifunctional, cryptic, remote-controlled & -updateable malware
Controls
Preventive
Policies, laws, regulations, contract terms plus awareness & compliance enforcement
Network perimeter & internal controls
Prohibit email attachments, websites, apps, unregistered media/devices etc. (whitelisting)
Disrupt criminal networks & activities e.g. command-&-control & money laundering
Patching, patch management, version control, maintenance
DEP, SEH & other kernel controls
Code reviews
Detective
Antivirus software
IDS/IPS, SIEM, heuristics & anomaly detection systems
Forensics, reverse engineering ...
Corrective
Data, app, system & equipment backups
Incident management & response
Business continuity management including resilience, recovery & contingency
Alert users, support staff/pro's & managers