Management briefing on

Malware metrics

Executive summary

Measuring and assessing the malware (malicious software) situation is necessary to make sure things are running smoothly and is a prerequisite to making systematic improvements, where necessary. This briefing proposes several different kinds of malware-related metric to consider and discuss, selecting or developing the few that management feels would be most cost-effective.

Introduction

Given that we feel it necessary to cover malware every year in the awareness program, it should be obvious that we consider malware a significant issue, but how have we reached that conclusion? We routinely track public information sources such as malware incident news reports and antivirus company research reports, assessing malware risks and controls in broad terms to spot the global trends or trajectories. Understanding and managing malware in the specific context of the organization, however, requires additional information concerning malware–related threats, vulnerabilities, impacts, controls and incidents within the corporation, which is where malware metrics come into play.

Potential malware metrics

Malware threat metrics

Who is behind malware incidents? What kinds of people or groups are they? What are their objectives and motivations? How competent, determined and resourceful are they? How malicious or nasty are they? Although there are some statistics in this area (*e.g.* the number of criminal and hacker groups known to be actively using malware, and estimates of the number of people in each group *etc.*), anecdotes and general impressions from experienced people working in the field are probably just as valid, especially considering that the criminals, hackers and spies responsible for malware do their utmost to evade detection for obvious reasons.

A few journalists, information security, antivirus and law enforcement professionals have gleaned useful information by infiltrating hacker/criminal underground social networks, although the credibility and validity of that information can be questioned: it is possible they are deliberately being fed misinformation, and they may be generating propaganda or exaggerating things for their own purposes. Estimates of the global costs of malware incidents, or the costs per record compromised, are notoriously unreliable, not least because the researchers are often financed by antivirus companies and likely biased, while small nonrandom samples make the problem worse.

Different kinds of organization or industries (*e.g.* financial services, retailing, government and defense) and different functions (*e.g.* IT, Finance, Operations, Research and Development, Sales and Marketing, Human Resources) or levels within them (*e.g.* staff, junior management, middle management, senior management), undoubtedly face different malware threats. One way to assess and report on this would be to develop ‘heat maps’ showing the distribution of high, medium or low

Copyright © 2016 IsecT Ltd.

threats, with notes to explain the rationale behind the ratings. Another possibility would be a ranking or prioritization approach, showing threat levels for each part relative to others.

Malware vulnerability metrics

Measuring the organization's vulnerability to malware implies an appreciation of all the myriad ways that malware can infect and affect things, and some assessment of their relative importance. At a high level, a large, complex, multinational organization that makes heavy use of IT and the Internet and has obvious problems with governance and compliance is likely to have markedly different malware vulnerabilities to a small, simple, well governed and tightly controlled organization with limited IT …. however such crude generalizations may be distinctly misleading as even the latter organization still has vulnerabilities, and malware need only find one way in to cause an incident.

Another approach is to attempt to measure, track and hopefully reduce malware vulnerabilities in a given organization over time, for example using metrics concerning:

- Patching status for systems, with a particular focus on critical security patches;
- Antivirus software deployment, maintenance/updates and effectiveness;
- Malware awareness and response levels among workers, including incident avoidance and reporting;
- Measures of technical complexity and change.

Malware incident and impact metrics

The number of malware infections sounds like a straightforward metric, but it's not as useful as it appears. Does a Zeus Trojan infection on three machines on the same day count as three incidents or one? And are these incidents "worth" the same as an APT or ransomware incident? While it is possible to measure or estimate such parameters, the metric may not be cost-effective.

The proportion of attempted malware infections that succeeded would in theory be a guide to the quality of the preventive controls, but in practice it is also hard to calculate reliably and objectively.

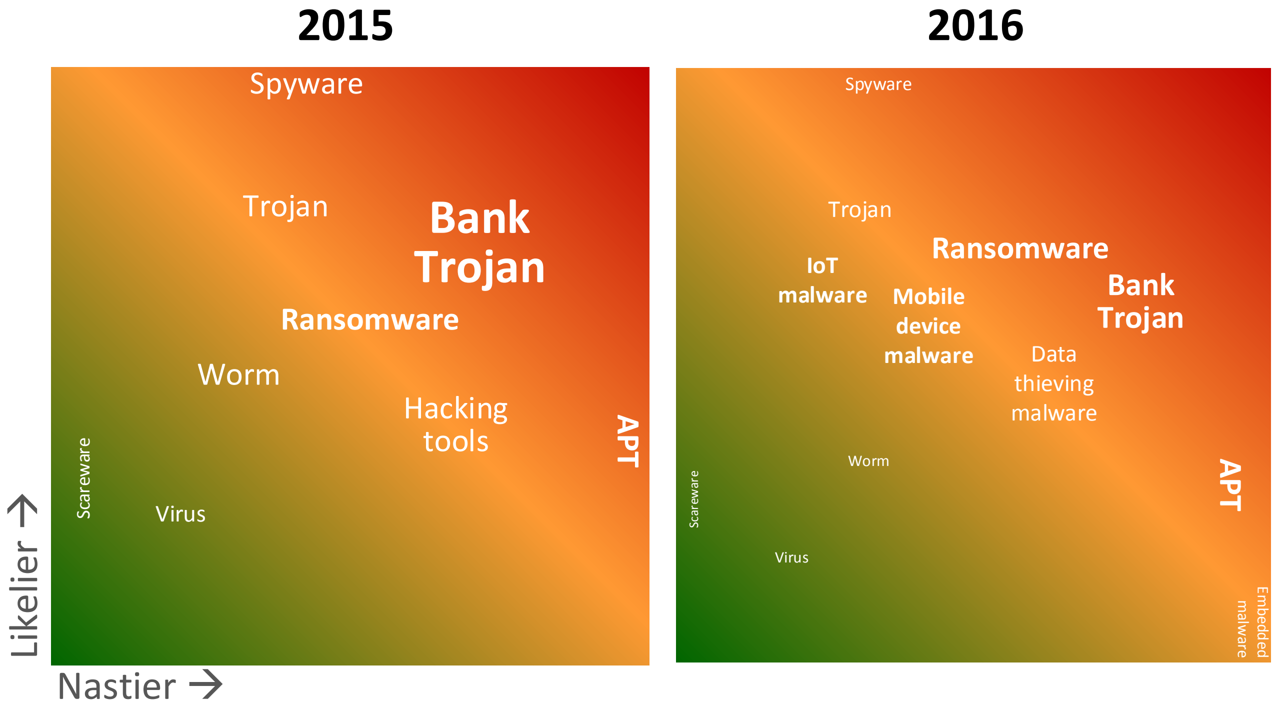
The costs relating to malware incidents may be measured or estimated through metrics such as:

- Man-days spent investigating and resolving incidents, plus associated costs for specialist assistance, forensics, legal experts *etc.*;
- Lost productivity and consequential business losses while infected networks and systems are taken offline, disinfected and restored (where possible);
- Direct losses due to fraud and theft;
- Other costs such as those arising from loss of/damage to data and systems that cannot be recovered;
- Intangible costs relating to loss of trust in the IT systems, fear of malware *etc*.

Malware risk metrics

The combination of threats, vulnerabilities and impacts is one measure of the malware risk. Analytical methods such as FAIR, FMEA and Mehari can generate impressive-looking risk metrics, although there is a tendency to place too much faith in numbers and pretty graphs derived from subjective assessments, categorization, invalid arithmetic and dubious statistics. As one of several means of risk assessment and decision support, though, they have their place.

Using the unashamedly subjective Analog Risk Assessment method, we have noticed changes in the malware risk picture during the past year:

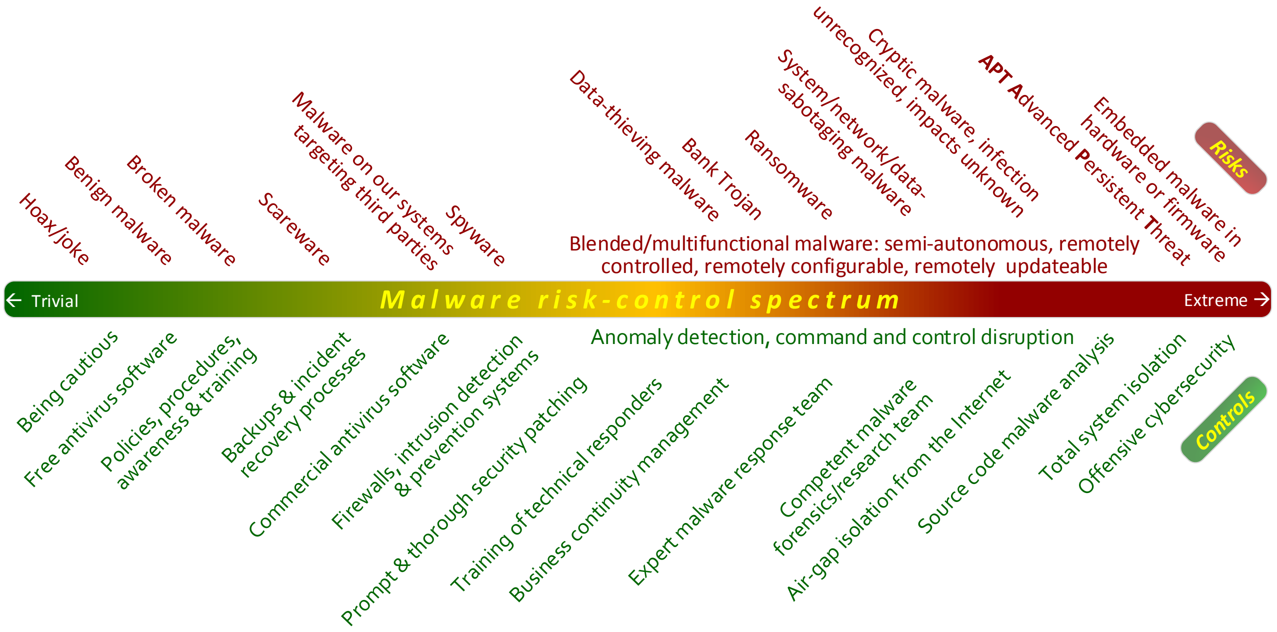


2015

2016

We have identified a few malware risks to demonstrate the approach and get you started. You may well disagree with their positions on the graph, and you should be able to think of other malware risks not yet shown: the key point is that this metric is a stimulating and creative way to compare, contrast and gain a better appreciation of the risks.

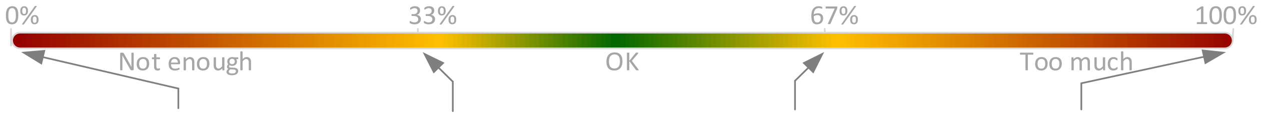
A spectrum diagram is a useful way to rank various malware risks and controls relative to each other, giving a rational basis for discussion and decision making around risk treatments:



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

Copyright © 2016 IsecT Ltd.

Malware-related maturity metrics



No malware controls	Weak malware controls	Strong malware controls	Excessive malware controls
No antivirus software is used, possibly because *someone* has asserted that it is 'completely unnecessary' and nobody has the expertise or guts to challenge them	Antivirus is installed on some but not all applicable systems, and is probably out of date on a substantial proportion of them	Antivirus is installed and updated on virtually all applicable systems, particularly the most important ones such as email servers, workstations and mobiles	Antivirus is managed using a state-of-the-art enterprise management system: 100% installed and totally current, with metrics and indicators being used routinely as part of the process
No IDS/IPS (intrusion detection and prevention systems) or SIEM (security information and event management) at all	Basic IDS is in place but barely functional: nobody feels responsible for it, the configuration is weak and alerts are usually ignored	IDS/IPS and perhaps SIEM is in use but resources are limited, consequently some low-level alerts are parked temporarily or permanently	IDS/IPS and SIEM are operating effectively, with sufficient skilled professionals to respond promptly and effectively to all valid alerts 24x7
Security patches are not routinely implemented	Some systems are security patched, if not always promptly	Most systems including all critical systems are promptly patched	All systems are always promptly patched, no exceptions
There is no appreciable awareness of or interest in malware – even the term is misunderstood	Some workers know something about malware, but not all and not much	Most workers know enough about malware, and relevant specialists have additional training	All workers fully understand and fulfil their obligations towards malware
There are no particular arrangements to deal with malware incidents, possibly no real incident management approach at all	There are basic responses to malware incidents, but they are neither effective nor efficient: basically malware response is *ad hoc*	There are specific response arrangements to deal quickly and effectively with malware incidents and/or outbreaks, with some evidence that they operate effectively and efficiently	A fully trained and tooled-up rapid response unit is primed and ready to respond to malware outbreaks or incidents – and the metrics indicate a highly efficient and effective record
Business continuity is an alien concept	Minimal, basic business continuity arrangements are in place but probably nothing specific for malware incidents, and probably poorly maintained	Reasonable business continuity arrangements are in place, with plans suitable for malware incidents, and some assurance measures such as tests or reviews	The organization takes business continuity, resilience, recovery and contingency seriously, with plans and arrangements routinely exercised and proven effective for a wide variety of incident types including malware

Copyright © 2016 IsecT Ltd.

Maturity metrics are constrained by the quality and nature of the scoring norms, plus the integrity and knowledge of those doing the assessment and scoring. On the other hand, they indicate the strengths and weaknesses of various aspects of the organization's approach relative to generally accepted good security practices, clearly implying that relatively weak/low-scoring aspects deserve more attention. Furthermore, maturity metrics of this style are very flexible: they can easily be updated and extended to track the evolving state-of-the-art, while giving the metrician sufficient latitude to reflect the reality of the situation on the ground, within reason: using the stated parameters as a guide, it should be possible to justify the scores against each of the criteria.

Conclusion

The malware metrics discussed in this briefing are merely suggestions to consider. Rating, comparing and contrasting metrics (*e.g.* using the **PRAGMATIC** approach), trialing potential metrics on a limited basis, and developing variant or novel metrics to address specific information needs, are suitable ways to select effective metrics. The whole process is much easier, however, if management first has a solid understanding of the organization's goals or objectives in relation to managing malware risks and controls, hence we recommend studying the other security awareness materials on this topic and discussing metrics with inputs from Information Security, Risk Management and IT.

For more information

Please browse the intranet *Security Zone* or contact Information Security.

Copyright © 2016 IsecT Ltd.