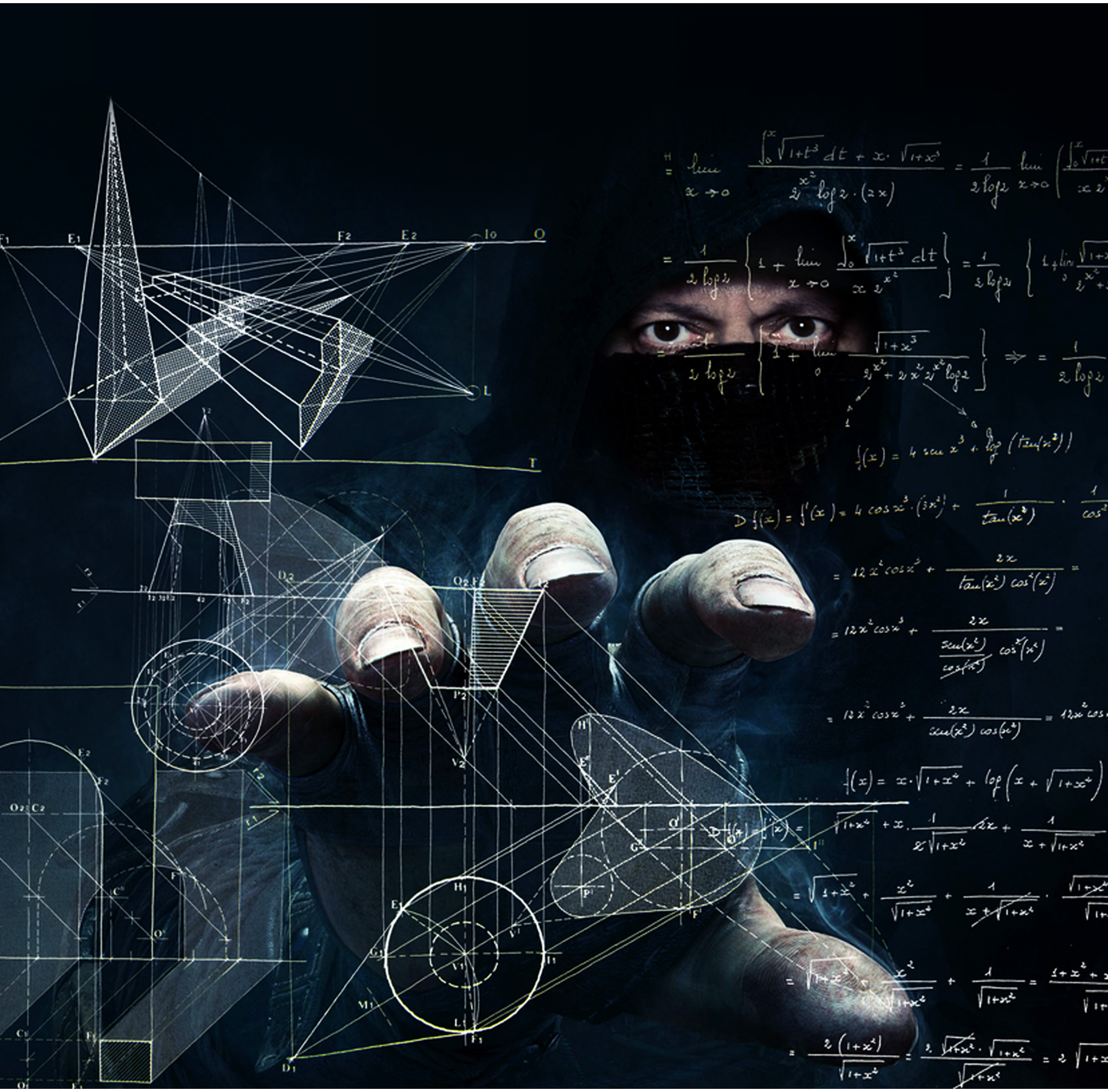
clearswift
RUAG Cyber Security

Protecting your organization from advanced threats

Prevent advanced Malware and Ransomware attacks from striking



Contents

Introduction

Today's cyber-attacks appear relentless, growing in frequency, intensity and proliferating throughout all industries. There is no 'normal' and the impact of each attack is felt throughout the business through the organization's supply chain to its customers, partners and beyond. It is almost impossible not to notice the cyber-security stories in the media. It doesn't seem to matter where you are in the world, or what industry you are in. But what has come to light, is traditional cyber-security protection is becoming increasingly ineffective against this next generation of ever evading malware and the myriad attacks.

Cyber-attackers have become patient. Mounting increasingly sophisticated campaigns against both organizations and the individuals within them using all the latest social engineering methods available. Silently harvesting information from social media platforms and hidden document metadata readily found on the company website or cloud collaboration tools, preparing for targeted attack.

To combat this onslaught, organizations need to deploy a more effective layer of advanced threat protection, aimed at securing their most valuable asset; critical information. Mitigating the new threat vectors of embedded malware in conjunction with supporting collaborative working practices, enabling the business to remain secure yet agile.

With a deeper layer of inspection and sanitization, the automated removal of hidden malware is the cornerstone to providing a more complete and cost effective solution to mitigating the new threats.

Are the number of threats really increasing?

For most CFOs, their favorite graph is 'up and to the right', unfortunately for the CIO when it comes to cyber-threats this is certainly not what they want to see. There was a 36% increase in unique malware in 2015 over 2014 which equates to 430 million instances[1]. But numbers are difficult to get to grips with, it is the impact of the malware on organizations which is easier to relate to.

The next generation of evading malware

Today's cyber-attacks are not just after credit cards or bank details, they are also targeting critical information. The information could be new product designs or personnel records, contract information or customer details. Critical information takes on many forms, and is pertinent to each organization, but each guise of critical information can be monetized very easily on the dark web or simply for the attackers own personal gain or held hostage for ransom.

Spear phishing

Most people are aware of phishing; an email which appears to be sent to you from a friendly source which you then act upon, creating the problem. This could be opening an attachment or clicking on a link - both resulting in a malware infection. Spear phishing is very similar but it is an attack which targets an individual or group of individuals with content which is very specific. Rather than a blanket approach of 'you are a customer of grocery store X, click here for a super deal', it's a crafted attack using personal references.

A recent spear phishing attack[2] targeting the US Nuclear Regulatory Commission (NRC) used employees' personal email accounts as the attack vector. There were three vectors used, a PDF attachment with malicious active content, a link to a document hosted on Microsoft OneDrive which was malware and a link to a Google docs spreadsheet also containing malware.

Today nearly 80% of spear phishing attacks use employees' personal email and other mail accounts rather than directly through corporate email. This route is chosen, as often corporate email accounts are better protected than personal email, which is delivered over the Internet.

[1] Symantec Internet Security Threat Report, April 2016
[2] www.theregister.co.uk/2014/08/19/nuclear_facility_hacked_three_times_in_three_years/

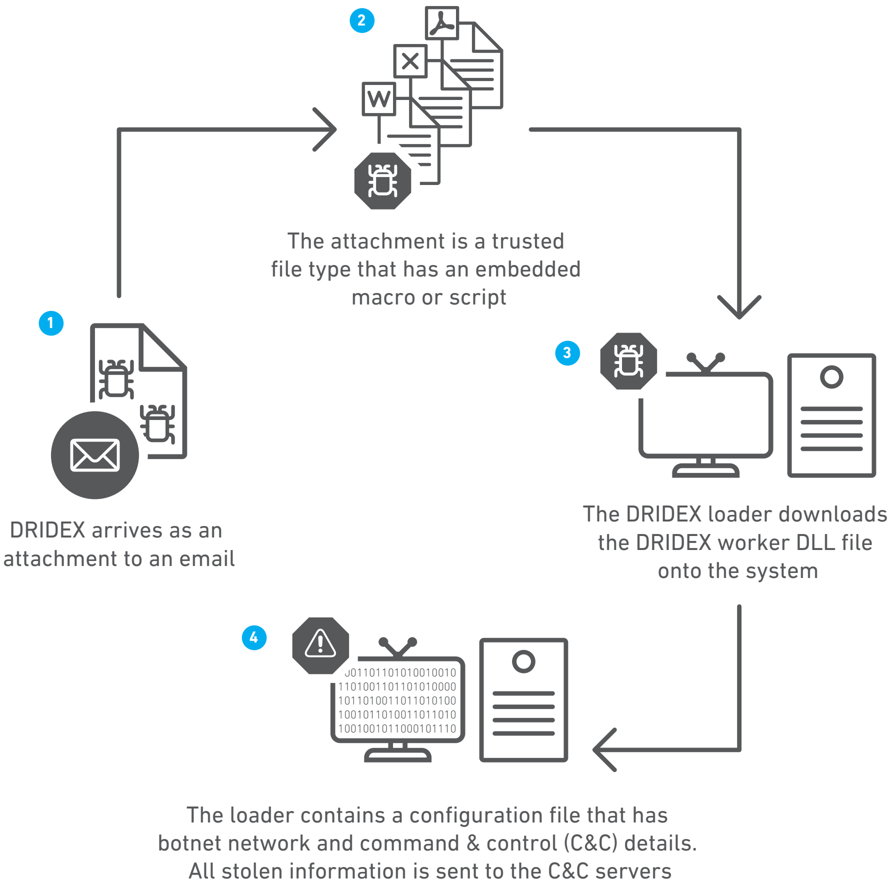
Ransomware

Ransomware is the latest branch of malware to move from being a consumer to enterprise blight. Rather than having to exfiltrate information, the malware encrypts it in place and then displays a demand for money. There has been a spate of attacks, particularly in the healthcare vertical with the Hollywood Presbyterian Medical Center[3] being one of the most recent and high profile. In this case the ransom demanded was $3.6M, but the real challenge for the organization was that computer systems were shut down for days whilst the medics were forced to use fax, pen and paper, causing a massive decline in productivity. Furthermore procedures had to be postponed, which not only created a short term issue, but ultimately will impact the organization's reputation.

These attacks are not localized but global, with attacks on German hospitals[4] and a New Zealand District Heath Board[5]. Likewise, while healthcare was targeted, attacks have been reported across other verticals, including local government.

For today's business, ransomware is a real threat and has evolved so that the outcome can be Potentially devastating. Ransomware is just a process and infection is as simple as 1,2,3. One recent example is DRIDEX, see Figure 1.

Figure 1: Ransomware through DRIDEX malware



DRIDEX arrives as an attachment to an email

The attachment is a trusted file type that has an embedded macro or script

The DRIDEX loader downloads the DRIDEX worker DLL file onto the system

The loader contains a configuration file that has botnet network and command & control (C&C) details. All stolen information is sent to the C&C servers

[3] www.itgovernance.co.uk/blog/major-hollywood-hospital-brought-down-by-a-ransomware-attack/
[4] www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030
[5] www.nzherald.co.nz/wanganui-chronicle/news/article.cfm?c_id=1503426&objectid=11594628

Evolution of attacks

The early hackers were motivated by fame rather than fortune and the targets used to be high-profile 'trophy' organizations.

The next round of hackers went after the low hanging fruit, information which could be easily monetized, credit card details and then bank account details. The value here was the immediacy of the monetization and an industry grew up around being able to process the stolen information as quickly as possible.

After credit card details, came other personally identifiable information (PII) which could be used for identity theft and hence monetization through impersonation. Medical information is now worth ten times more than credit cards. Usernames and passwords can also be monetized with demand for corporate credentials as well as consumer.

Today we are at the point where all critical information carries a value – to someone – and so is now a target, or in the case of hacktivists, it is about disruption (who also deploy other attack mechanisms, such as Distributed Denial of Service, or DDoS attacks.) Thanks to the Internet, there are no boundaries, the perpetrators are no longer just individuals who are out for 'fame', but rather larger groups, from hacktivists to organized crime to governments themselves (allegedly![6]) and can be based anywhere on the planet.

The attack vector has moved on from expecting someone to open an executable in an email, to clicking on a malicious link, to today's malware which is now embedded in innocuous looking documents. Open the document, infect the machine. Infect the network. This malware is almost impossible to detect using traditional mechanisms as it has been crafted for a specific individual or organization, evading even next generation firewalls, anti-virius and sandbox solutions. Once installed it operates 'low and slow', carrying out its task over a period of time rather than instantly, in order to avoid detection and is most frequently referred to as an Advanced Persistent Threat or APT.

What are the options to mitigate APTs?

Information borne threats are particularly difficult to mitigate against. In essence the malware is embedded into the document – but the document can also contain information which is actually required for legitimate business. For example infecting documents stored in a cloud based collaboration repository so that their payload is delivered when they are opened while on a corporate network. Cloud based collaboration is now the defacto standard when working with other organizations but due to lack of control, they can become the weakest link in the security chain.

What about sandboxing?

APTs are seldom detected by traditional anti-virus solutions, detection can be improved by using multiple AV engines, however even this is not 100% effective. Another approach is to use a sandbox. This is where the executable is run, or the document is opened in a controlled environment, a sandbox, and its behavior monitored. The major disadvantage of this approach is the ever-increasing sophistication of the malware which can now evade detection in sandboxes[7].

> *"Malware sandboxes have registered good results and potential in curbing the problem; however, authors of the malware have found ways of bypassing the analysis measures put in place. It is sound to say that sandboxes no longer provide or guarantee the needed protection that required to be afforded computing systems to prevent against malware attacks."*[8]

Sandboxing's secondary impact is the delay in delivery while the behavioral monitoring is taking place. Business communication is frequently time critical, especially those with documents attached (which is why people tend to open them before considering where they came from, and who might have sent it), so any delay is a delay to business. Organizations' who deploy sandbox technology often switch off the technology to ensure that the communication is delivered immediately and then take a copy for analysis. If malware is detected, they then have a process to try and delete the offending document before it infects the organization; the remediation often being too late.

[6] www.nextgov.com/cybersecurity/2014/08/exclusive-nuke-regulator-hacked-suspected-foreign-powers/91643/
[7] www.doctorchaos.com/malware-sandbox-and-breach-detection-evasion-techniques/
[8] www.sans.org/reading-room/whitepapers/forensics/detecting-malware-sandbox-evasion-techniques-36667

What about a dual anti-virus solution?

Most companies today have an anti-virus solution of one sort or another. Best practice is to have different vendor solutions on the ingress points to that which is on the endpoint. The reason for this being that each will detect viruses slightly differently, especially through heuristics. While it is not practical to have multiple AV solutions on each endpoint, it is on the ingress points, the email and web gateways. Using more than one solution improves detection by up to +19.2% on recently discovered viruses. Over time, all the anti-virus engines will detect the same viruses, but it is that additional coverage when a virus is first discovered which makes dual anti-virus effective.

What about next generation anti-virus?

Anti-virus solutions are only as good as the virus signatures and heuristics that they support. Signature updates from most vendors happen multiple times during the day and are automatically downloaded. However, there is the time from when a virus is detected to when the new signatures are installed. The next generation of anti-virus solutions enable a cloud-based lookup which makes the new signatures available in the time before it is downloaded as an update. This does reduce the risk with the reduction of the window of opportunity for the cyber-attacker, between the release of the virus and it being detected and blocked. However, fundamentally, the risk still exists.

What about Clearswift? Why is this approach different?

Clearswift has built its reputation on a technology called Deep Content Inspection, this is the ability to take a document or an archive and pull it apart and then analyze the constituent pieces. Further innovation came in 2013 with the launch of Adaptive Redaction and with it the ability to rebuild documents having removed any data which breaks information security policies. While the technology was originally developed as part of an Adaptive Data Loss Prevention solution, it has been refined to additionally deliver an easy to use, cost effective, advanced threat protection solution. The key component being Structural Sanitization.

Structural Sanitization from Clearswift

Deep Content Inspection (DCI) is used to fully understand a document and its constituent parts in real-time. When it comes to protecting against APTs, it is primarily about detecting and removing active content. These are embedded macros and scripts which activate when a document is opened. It can also look for and remove piggybacked content which is attached to other embedded objects, such as images.

In order to be effective, DCI doesn't stop at one level, it recurses through until an end is found[9]. So if there is embedded malware in a spreadsheet which is embedded in a word document which is in an archive, in an archive, then DCI will find and remove it. Unlike anti-virus solutions, it doesn't rely on signatures and doesn't require constant updating.

Structural Sanitization can be rapidly deployed and typically costs less than a fifth of sandbox technology. It requires no specialist training and does not impact business agility. It can also be combined with sandboxing, enabling a safe version of the document to be delivered while analysis takes place, at which point the original can be forwarded on if there are no threats detected. Furthermore, active DCI within the email (or web gateway) can ensure that only documents with active content are forwarded to the sandbox solution, reducing the overhead of the sandbox scanning innocent files.

[9] The default number of levels to recurse through is 50, at which point the policy can quarantine the content – as it is most probably malware.

Document Sanitization from Clearswift

Today's documents contain other threats embedded in them, outside of the obvious information, appearing in the guise of meta-data.

Metadata is the detail available to users that provides more insight into information; for example it will describe where information was created (such as GPS information in photographs or the name of the computer a document was created on) and hence the location of individuals can be tracked. It might provide details about authors, time and date of creation of information, amongst other property based description. This information is a gold mine for phishers and cyber-attackers – by providing the inside track to the organization which makes phishing all the more successful. Would you be more likely to open a document purporting to be from your IT department which has your corporate username as the title? Or maybe one referring to internal printer names? These innocuous looking pieces of data should never make it outside the organization, else it makes it easy for the cyber-criminal.

Another class of information hidden inside a document is the revision history. This might be obvious if you have 'track changes' switched on, or it might be embedded in the document by default, for example in fast save information. Either way, this can contain sensitive data which could result in a data leak.

Deep Content Inspection can identify meta-data and revision information and using Document Sanitization can automatically remove it, removing the threat it poses as it crosses the organizational boundary. This can be done through email and the web, for example when uploading documents to cloud collaboration platforms. Document Sanitization can also be used in front of an externally facing website using a configuration known as a 'reverse proxy', whereby any documents at the start of the download process can be checked and metadata or revision history which inadvertently remains is automatically removed before being delivered to the requestor.

Distributed Operational Management

As with any security solution there is often a management overhead. For many solutions this administration falls to the IT department or other system administrators. The Clearswift DCI technology is not restricted to understanding the content in documents (or emails) but also to the context, the sender, the recipient and the means of communication. Integration with Active Directory or an LDAP service enables the solution to route simplified management tasks to the sender's manager or any other nominated group or individual.

In summary

Organizations are under constant attack from today's advanced malware and ransomware attacks, with the proliferation urgently requiring a new approach to overcome the problem. As the attacks are becoming increasingly sophisticated and evasive, there is a need to rethink the defenses used. Unfortunately there is no silver bullet, so this is about augmenting existing defenses rather than just replacing them.

Structural Sanitization offers organizations effective mitigation against the information borne, evading threats. Automatically removing malware and ensuring there is no piggybacked data. Document Sanitization ensures that no critical information is leaked via metadata or revision history or identifiable information which can then be used by cyber-criminals to build spear phishing attacks against the organization.

A Sanitization approach is a cost effective solution to augment sandboxing techniques, traditional anti-virus, dual and next generation anti-virus, IP reputation, intrusion detection and other security applications to build a comprehensive defense-in-depth architecture; applicable for organizations of all sizes, in all industries to secure against today's advanced threats.

clearswift
RUAG Cyber Security

Clearswift is trusted by organizations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption and enabling organizations' to have 100% visibility of their critical information 100% of the time.

For more information, please visit **www.clearswift.com.**

United Kingdom
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading
RG7 4SA
UK

Germany
Clearswift GmbH
Im Mediapark 8
D-50670 Cologne
GERMANY

United States
Clearswift Corporation
309 Fellowship Road
Suite 200
Mount Laurel, NJ 08054
UNITED STATES

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
JAPAN

Australia
Clearswift (Asia/Pacific) Pty Ltd
Level 17 Regus
Coca Cola Place
40 Mount Street
North Sydney NSW 2060
AUSTRALIA