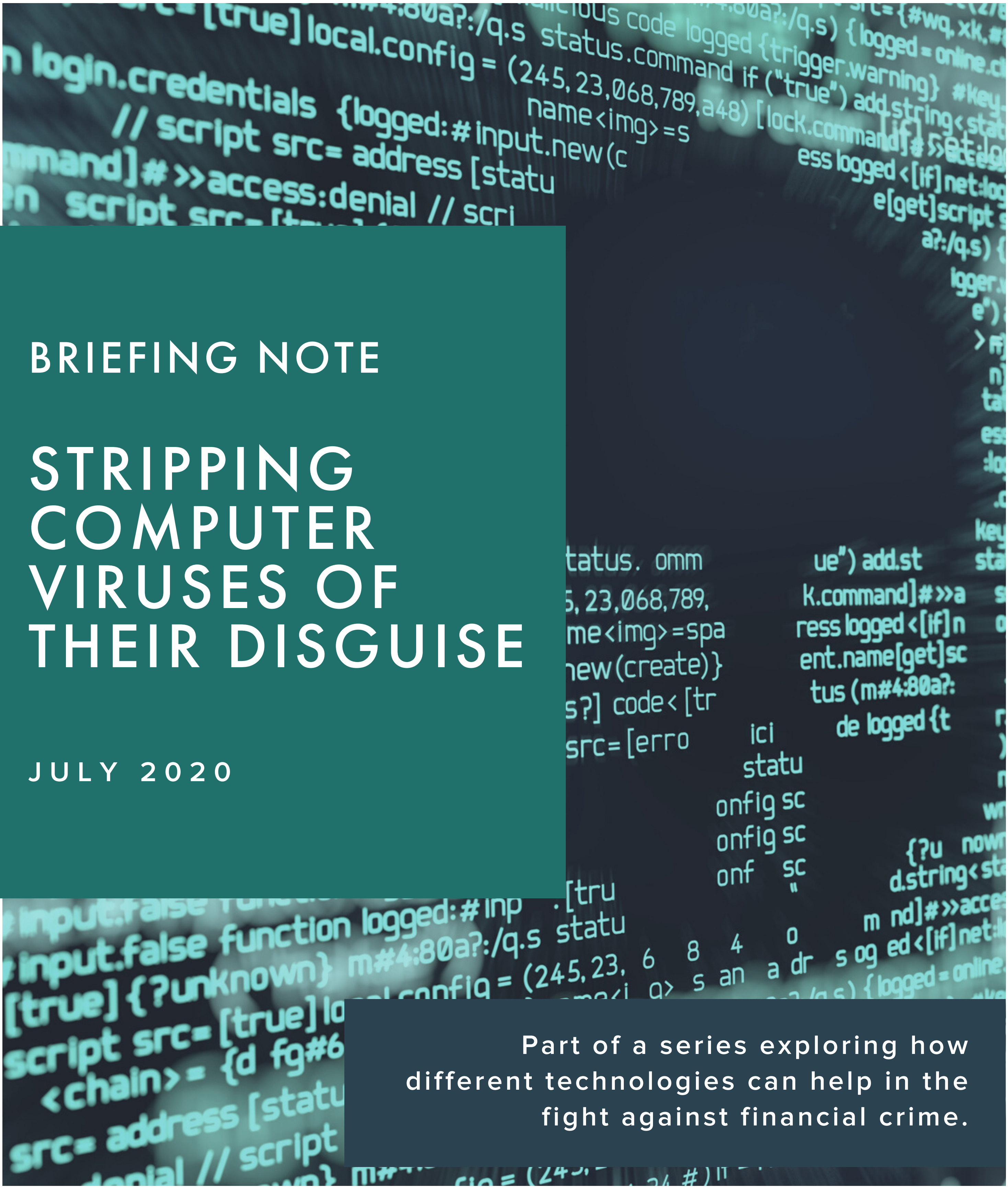


BRIEFING NOTE

STRIPPING COMPUTER VIRUSES OF THEIR DISGUISE

JULY 2020

Part of a series exploring how different technologies can help in the fight against financial crime.

THINK TANK | COMMUNITY | ADVISORY | TECHNOLOGY | OUTSOURCING

www.crime.financial

THEMIS

THE PROBLEM

On 25th June 2020, two months after launching its Suspicious Email Reporting Service, the UK's National Cyber Security Centre announced it had received over a million reports of attempted phishing attacks. These e-mails contain viruses which can cause a host of problems for those on the receiving end.

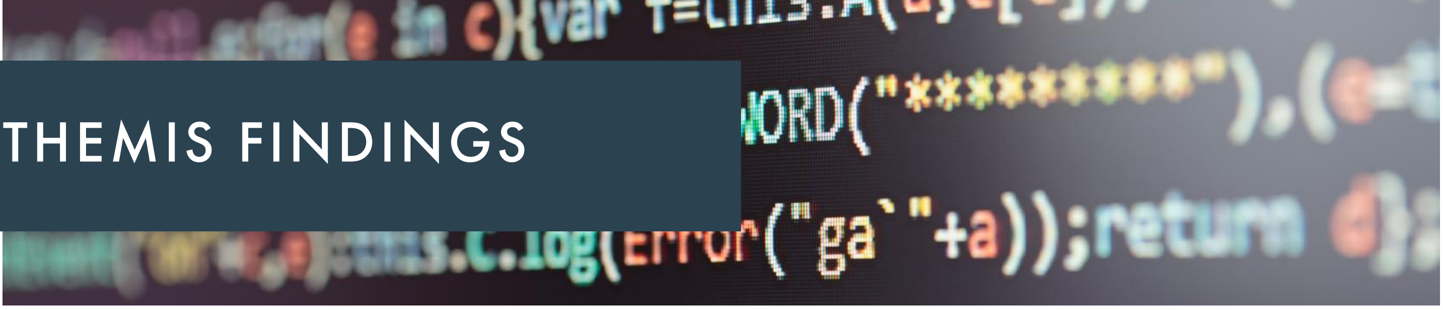
For businesses, these can include being subjected to ransomware (blackmailing a company by locking it out of its vital data), remote access trojans (where a criminal is able to take over an infected computer) or gaining access to a company's systems and downloading its critical data which can then be put up for sale on the dark web. Such is the scale of the problem that the FBI estimates that between June 2016 and June 2019, businesses lost $26 billion globally through e-mail compromises.

While the firms who find themselves victims to these attacks face significant financial and reputational loss, they are also likely to find themselves in the regulators' sights. According to the Financial Conduct Authority's director of supervision, Megan Butler, "we expect you to understand your vulnerabilities, invest in protecting those and protecting yourselves, consumers and the market."

The FCA, PRA and BoE issued a consultation paper in Dec 2019, which illustrates guidelines that are required to be followed by financial institutions in order to ensure they are operationally resilient.

Operational Resilience planning enables a bank to continue business knowing they have control in place if the business was faced with downtime due to IT disruption or natural disasters.

As cybercriminals become more sophisticated, earmarking their victims with malicious files, scattergun phishing attacks, or more targeted spear phishing (using social media and publicly available information to tailor their bait to the intended victim), or even whaling which seek out high level corporate targets, cybercrime represents a risk to businesses both from loss of earnings and the regulatory fines for losing customer data when systems are breached.



THEMIS FINDINGS

In one of our latest webinars exploring the use of different technologies to tackle cyber crime, Danny Lopez, CEO of Glasswall, stated that "The industry of cybercrime has changed dramatically. It’s recently been valued at over $1.5 trillion. If it was a country it would have the 13th highest level of GDP. It is now more significant than the drug trade for organised crime groups."

While companies are increasingly aware of the threat to their businesses from cybercrime, they are often unsure as to the best mechanisms to address the issue. In a survey conducted by Themis which asked senior financial services professionals to rate their biggest financial crime concerns across a range of threats from money laundering to terrorist financing, cybercrime came out by far as the leading issue facing businesses. “Cyberattacks are a real threat now with criminals using technology to create damage to the financial system,” was one of the typical responses from those surveyed.

Overall, 69.5 % of senior financial services professionals described cybercrime as their biggest financial crime concern echoing the scale of the problem as outlined by the UK’s regulator. Furthermore 30% of those surveyed confirmed that they had been exposed to cybercrime in the last 12 months with some noting, “the increase in phishing attacks,” as being a particular worry.

“When we broke down our survey results by job title we discovered cybercrime is an issue which CEOs and boards are particularly concerned about. For many we also got the feedback that it was somewhat outside of their comfort zone and expertise, making them feel increasingly vulnerable,” commented Dickon Johnstone, CEO of Themis.

This concern over cybercrime was also matched by a sense that their company’s current software was not up to the task of protecting systems from the criminals. One manager described their fears over, “the use of legacy systems which are easily circumvented by malefactors,” while overall 45% of the respondents believed that there was a significant cybersecurity gap in their systems technology.

This gap in companies’ systems has its roots in a number of problems both from companies themselves and from the software providers. Hence it is worrying that according to the Themis survey one problem was a perceived lack of innovation from established technology companies, “Technology providers are too slow or not interested in catching up or pioneering,” commented one respondent, while another complained of “awful” after service from vendors.

Another issue for companies is educating their employees about the cyber-risks they face, particularly when working from home, as well as businesses being able to acquire tools which can be used across a company’s entire workforce. “We require a holistic integrated set of tools which are efficient, effective and dynamic,” explained one respondent. Another commented that even with the correct software there was a pressing concern for employee education, “to ensure enough people across the company understand the systems and tools available to them and to apply them correctly.”

PREVENTION IS BETTER THAN CURE

"The criminals today are super organised and they treat cybercrime as a commercial activity. They have support, research and development, some of the best levels of service in the world are for the Bitcoin scammers for instance," said Dinis Cuz, CTO Glasswall, in our recent webinar - How Antivirus won't save you - Is CDR the answer?

To counter the ever-changing tactics of cybercriminals, security professionals have started targeting a strategic weakness of viruses, which is that these files will necessarily be dissimilar to the code around it. Previously security systems relied on viruses being identified, typically after they had already been known to cause damage, and then patching software to spot this code and to avoid it.

With a new computer virus estimated to be created every 4.2 seconds, the sheer scale and ingenuity of cyberattacks makes these catch and kill operations increasingly less viable, while systems are potentially unable to recognise computer viruses which are yet to be discovered. As the UK's National Cyber Security Centre observes, "Patching reduces the risk of compromise from known vulnerabilities, but it does not address the risks posed by an attacker with knowledge of vulnerabilities which aren't in the public domain."

Instead, government agencies and now the private sector have been making use of a band of technology known as Content, Disarm & Reconstruction (CDR). This technology interrogates external data being sent into a network, for instance via an e-mail to an employee or web browsers, and breaks files down into individual components.

The software then reconstructs these files having removed any abnormalities or deviations from the file's prescribed structure and sanitising out risky Active Content such as Macros and embedded files which have not been pre-approved by the system administrator.

Traditionally, "A lot of this technology was built when all of the threats were known. It's always a race to identify threats before bad actors use them. The problem you have now is there is so much malware out there. The attack vector has become much much bigger. So CDR takes a concept which has come out of the intelligence world – it confirms whether a source is genuine rather than seeking to identify an individual threat." said Simon Church former Chief Executive of Vodafone Enterprise security services and Glasswall advisor.

PREVENTION IS BETTER THAN CURE

CDR technology is therefore able to protect systems from the most sophisticated forms of cyberattacks including so-called zero-day exploits, the blue chip computer viruses which are stockpiled by governments and criminals and which are so potent primarily because they have never been used (and therefore never identified) before.

In fact CDR was developed by Western intelligence agencies to protect from the kind of state-sponsored threat presented by countries such as North Korea who are estimated to have funded the country's illegal weapons program to the tune of $2 billion through cyberattacks on banks, or Russia's targeting of critical national infrastructure in countries it deems a threat.

Allied with reliable threat intelligence reporting, a good CDR system is also able to spot increased levels of attempted breaches, normally a precursor to a business being subject to a more serious attack.

However, CDR also prevents less headline grabbing cyberattacks. Research by Glasswall has identified that among the most common vectors of cyberattacks on businesses are doctored PDF documents, but in an effort to thwart this threat, many anti-virus technologies adopt an aggressive quarantine posture, holding back files suspected to be malicious, but which are perfectly benign. This 'false positive' phenomenon causes significant disruption to productivity. By regenerating all PDFs to a standard of 'known good', a sophisticated CDR system is able to ensure all files entering an organisation are made safe without holding back documents that users need to do their jobs.

"It's important to remember that there is no silver bullet. Training is important, anti-virus is important. CDR complements all the above. It is a layer of security and as the criminal actors continue to develop their technology we need that complementary layered security strategy and CDR plays an important role in that." Danny Lopez CEO Glasswall.

CONCLUSIONS

With criminals locked in a game of cat and mouse with security providers, seeking to exploit any holes in company's software before they can be identified and patched, CDR offers businesses a chance to proactively protect themselves both from current and future cyberthreats. This is particularly important in an environment when regulators are expecting companies to protect their clients' data and this same data is deliberately targeted by cybercriminals.

A recent attack in the USA illustrates this point: In late June 2020 it was reported that the University of California San Francisco had paid a $1.14 million ransom to hackers who had accessed their systems and encrypted all their data. During the negotiations over the ransom payments it was apparent that the criminals had also helped themselves to the university's datasets. "You need to take us seriously," wrote the hacker in a live chat on the dark web. "If we release student records/data on our blog I am 100% sure you will lose more than our price what we asked."

Similarly, in 2018, within minutes of British Airways being hacked details of some of the 500,000 individual's data which was stolen was being traded on the dark web. The company was later fined £183 million by the Information Commissioner's Office.

The spoils presented by these breaches and the inventiveness of cybercriminals has meant that all companies are potentially in danger from both loss of earnings and large fines from regulators.

However, CDR changes the terms of the relationship. While criminals will always look to new ways of attacking companies, at a base level viruses depend on being wolves in sheep's clothing. Businesses armed with the right technology, now have the chance to make them look increasingly naked.

If you or your organisation would like to understand more about the latest developments in cyber security and where this software can fit into your existing systems Themis would be happy to help. Please contact one of our team to find out more:

Sandeep Sroa
Associate Director
sandeep.sroa@themisservices.co.uk
+44 (0) 7786 236 774

Henry Williams
Head of Investigations
+44 (0) 7780 746 290
henry.williams@themisservices.co.uk