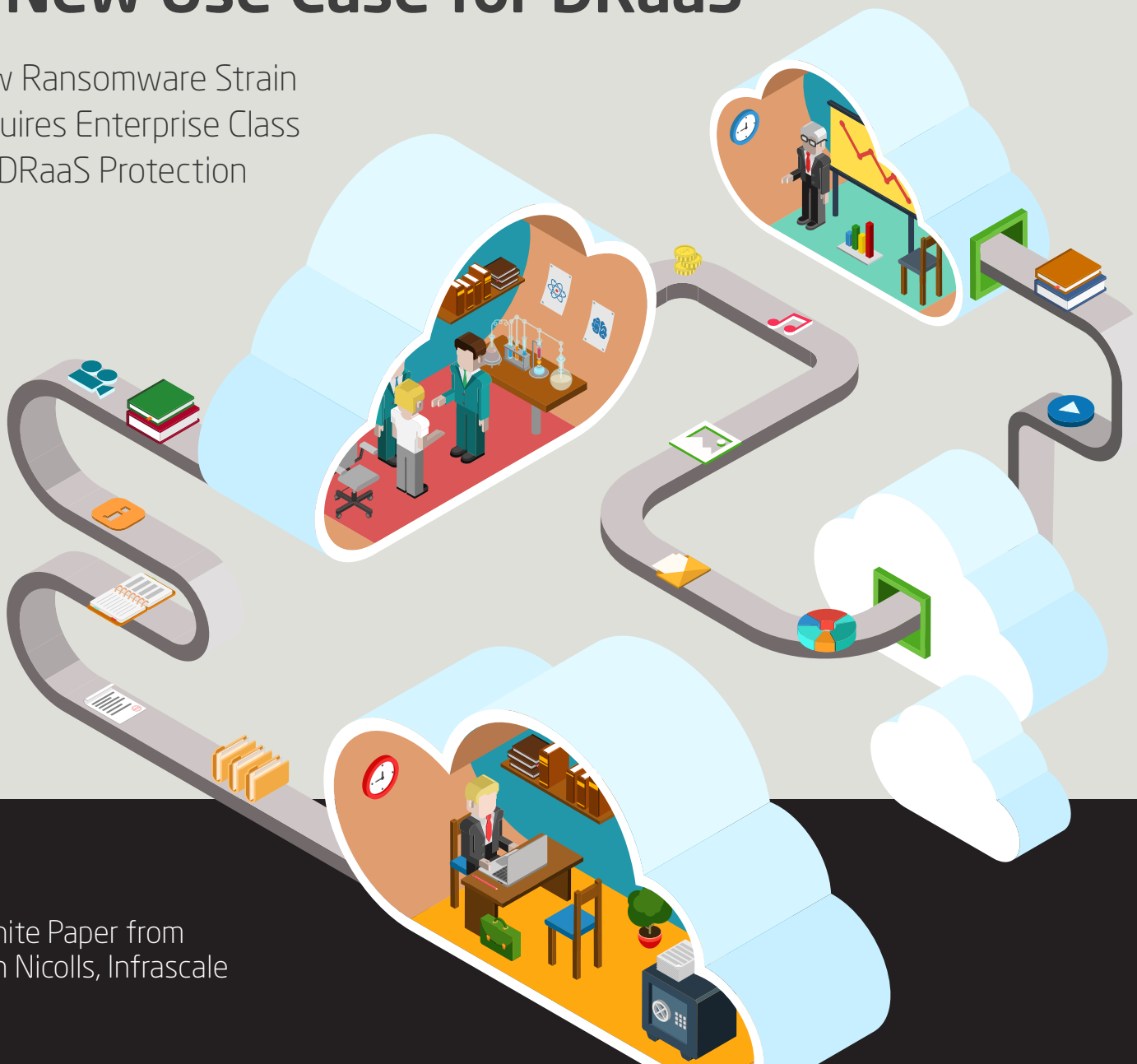
Infrascale™

Un-Locky for Business:

A New Use Case for DRaaS

New Ransomware Strain Requires Enterprise Class DRaaS Protection



A White Paper from
Dean Nicolls, Infrascale

Un-Locky for Business: A New Use Case for DRaaS

New Ransomware Strain Requires Enterprise Class DRaaS Protection

In the good ole days of ransomware, hackers only went after consumers and their individual files and folders. Older types of ransomware such as CryptoWall and CryptoLocker encrypt your individual files and documents when they infect a system. Much of the guidance provided by security experts has focused on removing the virus, but there are no known methods of getting your files back... except for paying the ransomers.

Over the last year, many of us have heard of the ransomware attacks that lock out a specific user from their files. Most of us assume this is just the latest in the ongoing battle between hackers and the anti-virus/malware companies. Eventually, we'll all be able to update our definitions and be safe to proceed as usual, right? Wrong. The growth rate of these infections are unprecedented both in terms of reach and in terms of money being lost by victims. There is no silver bullet so all users must be vigilant as they open emails, attachments, and webpages.

These strains of ransomware are increasingly targeting small businesses' systems and extorting payment from their victim for the decryption key.

Locky, for example, is one of the strains specifically targeting SMBs and is growing at an alarming rate. Locky encrypts files on victims' computers and adds a .locky file extension to them. Locky is different in other ways too, including its global impact, focus on businesses and non-profit organizations, and ability to spread to an entire computer network.

PHOTO: SHUTTERSTOCK

WORLDWIDE REACH

The attackers behind Locky have pushed the malware aggressively, using massive spam campaigns and compromised websites. One of the main routes of infection has been through spam email campaigns, many of which are disguised as invoices. Attachments disguised as word documents and other seemingly harmless files containing a malicious macro are used to trick users into releasing the virus onto their machines.

Since February 2016, Locky has spread by at least five different spam campaigns. Most of the spam emails seen had a subject line that read "ATTN: Invoice J-[random numbers]." Another campaign used "tracking documents" as a subject line. The spam campaigns spreading Locky are operating on a massive scale. Symantec detected more than 5 million emails associated with these campaigns.

This month, computers throughout Europe and other places have been hit by a massive email spam campaign carrying malicious JavaScript attachments that install

the Locky ransomware program. Many countries in Europe have been affected, including the UK, Luxembourg, Czech Republic, Austria, and the Netherlands. But Japan, New Zealand and Australia are also being targeted in similar spam attacks.

Closer to home, Amazon users have been targeted by a massive phishing campaign. It's estimated that 30 to 100 million spam messages claiming to be an Amazon.com shopping order update. The Amazon campaign is noteworthy in that the ransomware used botnets running on hijacked virtual and consumer machines.

TARGETING DEEPER POCKETS

Seeing the great success of early strains in 2014-2015, more and more hackers have entered the fray but with larger targets in their sights. Previously, ransoms amounted to a couple of hundred dollars (depending on the Bitcoin market rate) and was often paid out by the victim. But, with each day, ransomware attacks grow more agile, expensive, varied and widespread, and increasingly take aim at businesses of all sizes in all sectors, rather than consumers.

The value of your personal files and pictures has a finite and limited value. But, if the back-end of your corporate system is encrypted, preventing you from processing payments, the value of unlocking those files is exponentially increased. When the hackers recognize the value of what is being held ransom, the payment can be more dynamically set based on the content of the data.

It's clear that these hackers have been planning large-scale attacks for some time. It has since infected healthcare facilities throughout the U.S., the HQ of India's Maharashtra government, the Whanganui District Health Board Whanganui in New Zealand and the Chinese University of Hong Kong's Faculty of Medicine. While many of the targets have been healthcare organizations, businesses of all types are increasingly becoming attractive targets. This is especially true of SMBs who are less likely to have enterprise-grade malware detection and more importantly, adequate backups.

When the hackers recognize the value of what is being held ransom, the payment can be more dynamically set based on the content of the data.

Seeing the great success of early strains in 2014-2015, more and more hackers have entered the fray but with larger targets in their sights.

This is clearly not just a consumer play.

INFECTING YOUR ENTIRE NETWORK

Like other types of ransomware, Locky is designed to encrypt important files for the purpose of holding them hostage, but it has added a new twist. Locky has the ability to encrypt network shares and drives that your workstation may not normally have access to.

As of Spring 2016, 93% of phishing scams contained ransomware. The reason is simple: users are known for making mistakes or not being trained well enough to identify such attacks. With the single click of a mouse, a user can introduce ransomware software onto their system. Once a user has given a program permission and access to run, it'll be free to operate quietly in the background without the user noticing.

Locky and newer variants will travel through network drives to encrypt any files they can get to using the permissions from the original user account where the infection started. With Cryptowall, for example, the ransomware could only infect network drives that the PC was connected to (i.e., it could only reach the drives you had mapped on your computer). But because the Locky ransomware can encrypt any network shared drive, whether or not your workstation has access to it or not, it means the virus can spread to an entire business network.

DEFENDING AGAINST LOCKY

There are many articles available on how to prevent being a ransomware victim, including our own Enterprise Ransomware Survival Guide. Much of the standard guidance revolves educating your users about safe computing

practices, using enterprise grade antivirus software, and performing regular backups.

But Locky is special and requires a few extra safeguards because of the potential network impact, including:

- **User Training.** Training users on safety and identification of phishing scams is invaluable. There are even reports of companies experiencing "double" and "triple" ransomware attacks because different users kept getting different strains of the virus.
- **Admin Rights.** Don't give yourself more login power than you need. According to security software provider, Sophos: "Don't stay logged in as an administrator any longer than is strictly necessary, and avoid browsing, opening documents or other "regular work" activities while you have administrator rights."

Since users are the main entry point for ransomware, training users on safety and identification of phishing scams will be invaluable.

- **Edit your Firewall Rules.** Do not allow traffic from other countries unless you specifically need to allow that traffic. That will significantly reduce the amount of spam that hits your email servers and, as a result, dramatically reduce your chances of infection.
- **Anomaly Detection.** One of the many challenges with ransomware is the time delay between initial infection and the ransom notice. Once you're infected, the malware secretly encrypts your files (including those on network shares) and the user may not know that they've been infected, sometimes for months. Unfortunately, this is no early warning system that can alert IT to the infection. Until now.

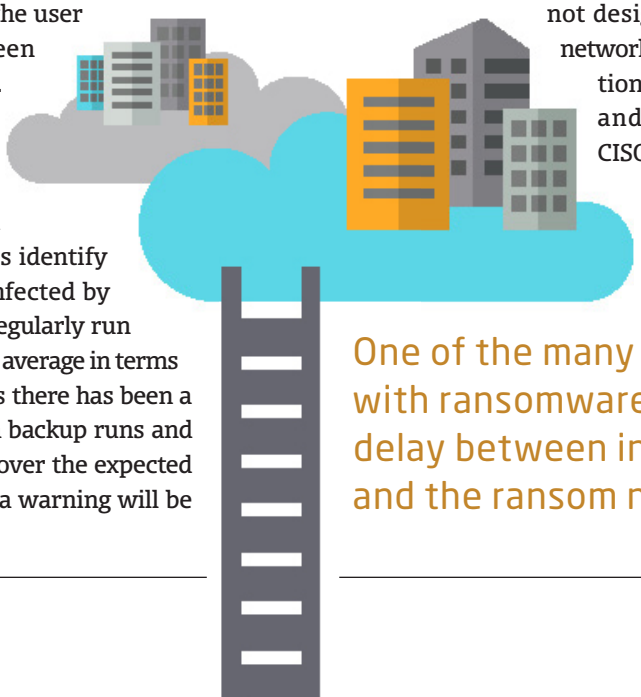
Infrascale has developed Anomaly Detection which helps identify whether you may have been infected by malware (e.g., ransomware). Regularly run backups should have a consistent average in terms of files modified or added unless there has been a significant event or change. If a backup runs and the number of files modified is over the expected average by the set percentage, a warning will be issued. With Locky, it's possible that all of your copies of an infected file may be infected and encrypted.

- **Unlimited Backup Versioning:** Many security observers have correctly noted that having a backup strategy is a sound insurance policy against ransomware.

Commonly, organizations place too much confidence in their antivirus software. But, that's a dangerous gamble.

If clean images of the infected machines are readily available, organizations can completely wipe the infected hardware and restore it to the last good version. But some cloud backup solutions only offer a limited version history (e.g., they may only keep 10 copies of a particular file on hand and not retain older versions) and this poses significant risk to your business. With Locky, it's possible that all your copies of an infected file may be infected and encrypted. That's why companies need to leverage a cloud (or offsite) backup solution that keeps an unlimited version history.

- **Patch early, patch often.** Malware that doesn't come in via document macros often relies on security bugs in popular applications, including Office, your browser, Flash and more. The sooner you patch, the fewer open holes remain for the crooks to exploit.
- **Disaster Recovery as a Service solution (DRaaS).** Enterprise grade ransomware demands enterprise grade data protection. With cloud backup solutions, you can restore individual files and folders, but they are not designed to restore entire networks. Modern DRaaS solutions backup files, folders, and VMs which enables CISOs and IT administrators to quickly restore and failover applications in minutes.



One of the many challenges with ransomware is the time delay between initial infection and the ransom notice.

WHY ANTIVIRUS PROTECTION ISN'T ENOUGH

Commonly, organizations place too much confidence in their antivirus software. But, that's a dangerous gamble. Here's why:

- **Antivirus is only 47% effective:** Antivirus software are signature-based and usually only detect known threats. It cannot quarantine and delete programs it doesn't know are a threat. With the flood of zero-day threats and stream of vulnerabilities pouring out of web browsers, plug-ins, and the Windows operating system, antivirus can only be part of a layered solution.
- **Crypting eludes known signatures.** Crypting (sometimes called metamorphic malware) is a type of iterative malware that is written so that each succeeding version of the code is different from the preceding one. The code changes makes it difficult for signature-based antivirus software programs to recognize that different iterations are the same malicious program. The longer the malware stays in a computer, the more iterations it produces and the more sophisticated the iterations are, making it increasingly difficult for antivirus applications to detect, quarantine and disinfect.
- **Holes in your firewall:** Another question that's often asked is why your organization's firewall didn't catch the malware. A firewall only blocks incoming connections. If you close unused ports on your firewall you can do a pretty good job of keeping hackers from initiating connections to services on your network, however, the firewall doesn't block outgoing connections made by yourself or others.
- **Disabling antivirus protection:** Unfortunately, the actions of a few users can leave your organization exposed to infection. The reasons for doing this are varied: they may be installing new programs from the Internet or simply want to improve their Internet performance. Don't think this is real? Try Googling your AV solution and "disable" and see what comes up. Unfortunately, the actions of a few users can leave their organizations exposed to infection.

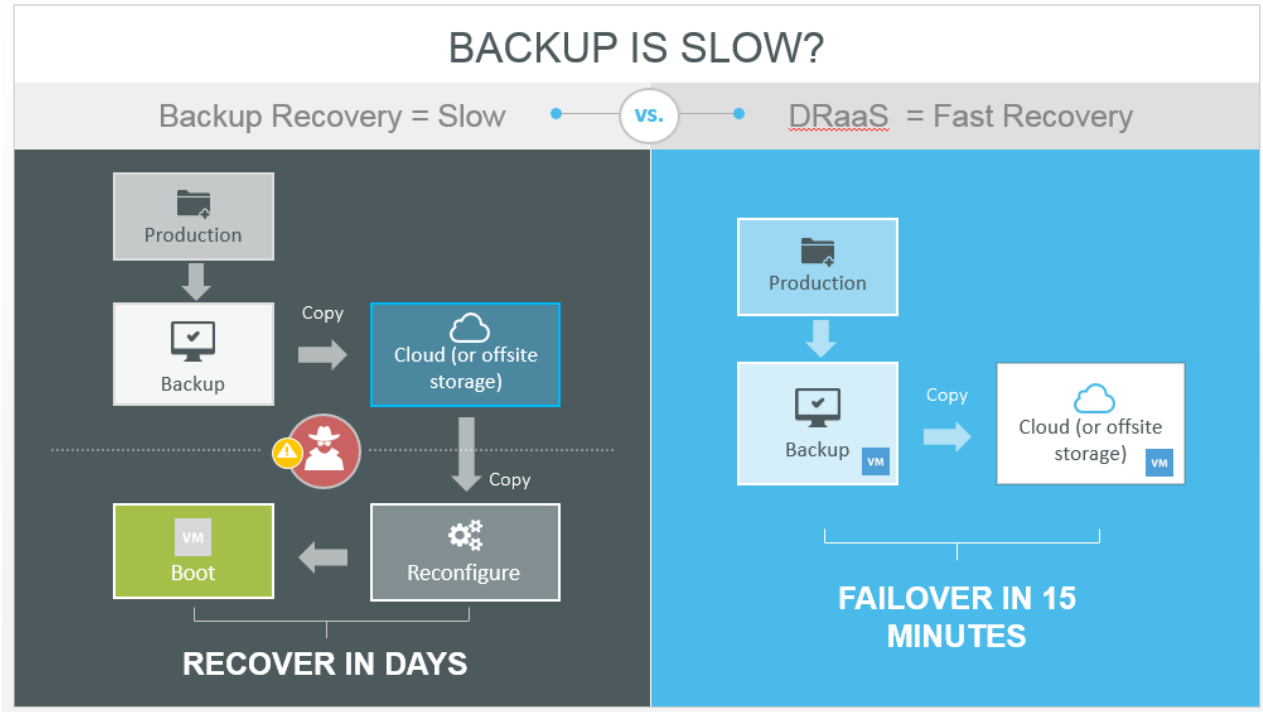
Does this mean antivirus software is completely useless? Not at all. Very often, your antivirus product will detect a new variant as something akin to a threat it has seen in the past. Perhaps the bad guys targeting your organization didn't use a crypting service, or maybe that service wasn't any good to begin with. But, it can't be the complete story.

DRAAS: YOUR SECRET WEAPON AGAINST LOCKY

Another challenge with ransomware is just how fast the malware can infect your files. In a recent study, it took Locky just 54 seconds to encrypt 1000 Word documents (70 MBs total file size) between execution and notification.

This has very real implications for traditional cloud backup solutions. If thousands of files – including application files - have been infected, then restoring these files from clean versions in the cloud will take time to download and reconfigure. And it's this time lag that can crush a business since the true damage of ransomware is not the actual ransom, it's the damage that occurs due to employee downtime, which can last for days, halting business operations and jeopardizing sales. That's where DRaaS (disaster recovery as a service) comes in. DRaaS is the latest evolution in cloud-based backup technology. DRaaS allows a user or admin to stand-up and recover an entire network in very little time versus limiting recovery to a specific set of users' files.

The longer the malware stays in a computer, the more iterations it produces and the more sophisticated the iterations are, making it increasingly hard for antivirus applications to detect, quarantine and disinfect.



By not having to copy data back to production and rebuild the infected machine, DRaaS can be a huge time saver to restoring productivity and peace of mind. With DRaaS, IT administrators can restore running systems (complete images) from backed up virtual machines in minutes from either a local appliance or the cloud. This lets your users stay productive, while your IT department can work to identify and eradicate the malware.

Another benefit of DRaaS, is that it lets IT admins more quickly identify the date of infection. With cloud backup solutions, you have to inspect individual files and folders to determine if they've been encrypted. If thousands of files have been infected, this can take a long time to isolate and pinpoint the date of infection. With DRaaS, admins can browse a disk image to more quickly determine if the files contained in the image have been encrypted.

This enables you to identify the date of infection so you can restore a clean copy of your data and applications from a date just prior to the infection. With traditional backup solutions, determining the date of infection and restoring clean copies of the infected files is a cumbersome and time consuming – with DRaaS, it's far easier.

THE BOTTOM LINE

Locky is a game-changing threat for businesses of all types. But thankfully, there are simple and cost-effective ways to protect your organization. It starts by teaching your employees and anyone who has access to your computer(s) about these safety regulations and make it a requirement that they learn the basics of cyber security.

With all of the malware threats that exist, every business needs to invest in enterprise-grade malware detection, disaster recovery as a service, and a few best practices in order to safeguard their data and systems.

With all of the malware threats that exist, every business needs to invest in enterprise-grade malware detection, disaster recovery as a service, and a few best practices in order to safeguard their data and systems.

We strongly encourage you to ask your I.T. department or consulting firm what precautions they're taking to protect you from ransomware. If you're not certain that your data and networks are completely protected, please contact us and we can help you evaluate your risk and make sure your business data and systems are as secure as possible.