WINTER 2017

THE SOURCE

Hints, tips, tools and resources from real IT geeks.

AWAY FROM PRYING EYES

Keep your network, data and users safe from whatever lurks in the dark.

IN THIS EDITION

Welcome to the Winter edition of The Source - hints, tips, tools, and resources for IT novices and experts alike.

In this edition, we look at keeping you safe online with some useful security tools, actionable processes and a dose of common sense. We also take a look at the future of Windows and get hands on with logging software and a great little disk array calculator.

I hope you find the magazine useful and if you have any other questions check out our blog, connect with us online or give us a call.

Sincerely, Jesse.

Jesse Rink
OWNER, SOURCE ONE TECHNOLOGY.

An experienced network engineer, Jesse has been sharing his expertise and experience with schools, non-profits and businesses in South Eastern Wisconsin for over 18 years.

CONTENTS

Subscribe to 'The Source' and get all the latest issues straight to your inbox.

sourceonetechnology.com/the-source

Source One Technology provides IT support to businesses, schools and nonprofits across South Eastern Wisconsin.

ALL YOUR DATA ARE BELONG TO US.

Malware evolution

THE TITLE IS A TWIST ON A POPULAR INTERNET MEME BASED ON A PHRASE FROM THE CLASSIC ARCADE GAME, **ZERO WING**. ONLY IN THIS CASE, IT'S NOT A GAME. IT'S YOUR DATA. IT'S WORTH MORE NOW THAN EVER TO MALWARE CREATORS WHO WANT TO PROFIT FROM IT.

Years ago, malware might have been a nuisance that popped open your CD drive or caused text on your screen to cascade into a pile of gibberish.

Over the years, malware evolved and began to exploit higher privileges to gain deeper access into your system. It became more difficult to detect and remove. Sometimes, it ironically disguised itself as an antivirus program, trying to compel you to pay for it.

If that wasn't enough, malware has evolved to the point where it holds your files for ransom—by encrypting them. You're not being scammed into buying fake software—you're being forced to pay to get your files back.

Crypto-ransomware, while nothing new, has been evolving over the years. Files on mapped/network drives, even unmapped shares, are being encrypted, causing chaos in corporate, multi-user environments. Some versions might replace the bootloader, crashing the system and leaving the user with a message that they've been hacked, their files are encrypted, and now they must pay.

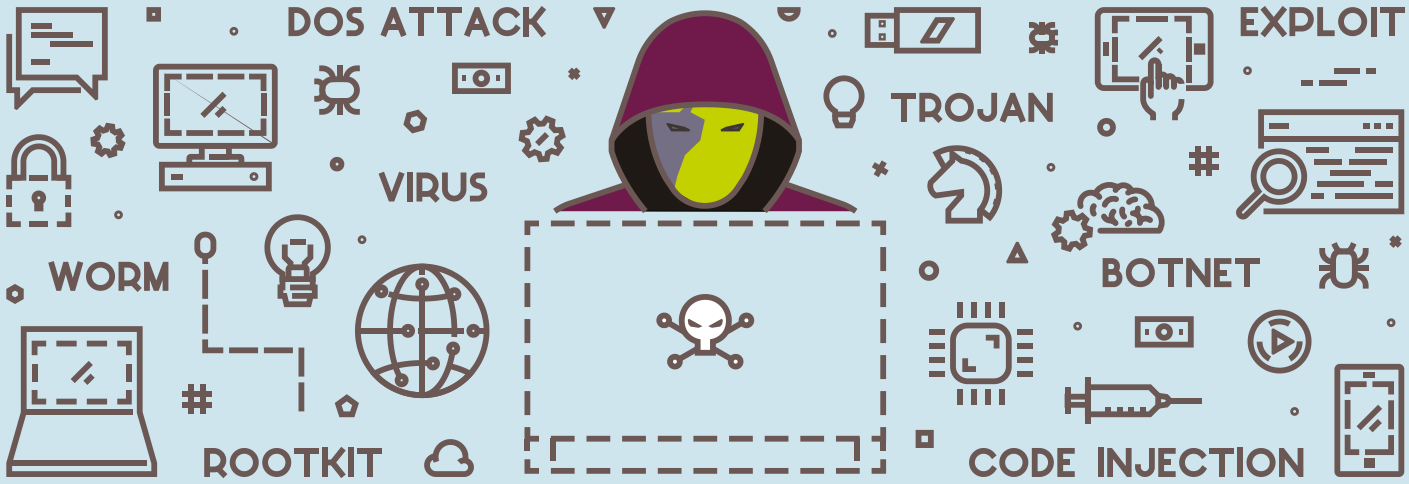
The endgame remains the same. But, that's evolving too. As the timer counts down to the payment deadline, the price begins to increase. The more you panic, the more the creator gains.

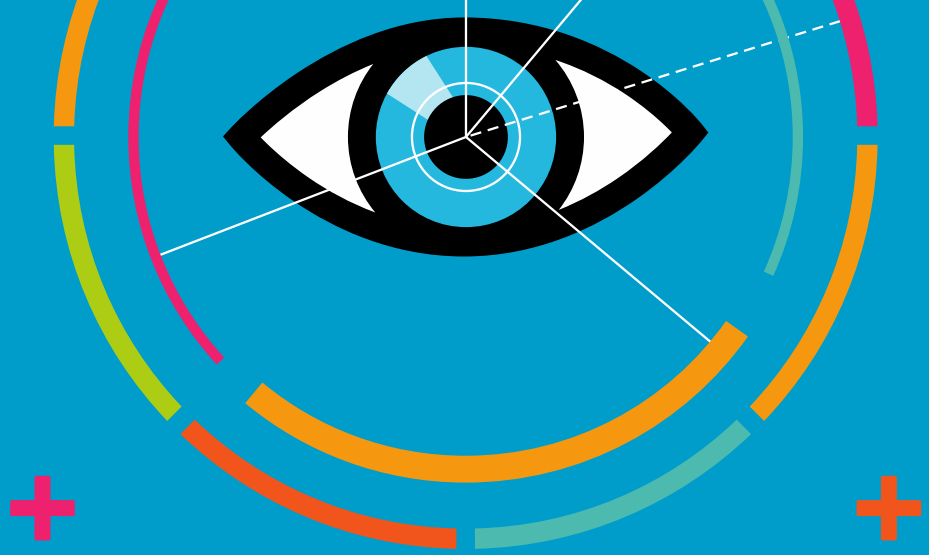
In response, many individuals and companies have beefed up their backup strategies. While this is great for many reasons, be aware that some of this malware has evolved beyond just encrypting your files and drives. It can harvest and upload email addresses, usernames, passwords and other files to rogue servers which the creator controls.

Because of this, the creator might now have deeper access into your network and company than you originally thought. Information about personnel, payroll, and even intellectual property might be worth more than a simple bitcoin payment from a victim.

There are many ways to prevent malware and ransomware infections, and if needed, recover from them. As malware continues to evolve, so must our prevention and defense against it.

Check out our blog for a great article titled **10 effective ways to minimize the risk of ransomware**, which includes guidance on defending yourself against ransomware and other malware attacks.





SECURITY

Password managers

Fingerprint readers. Voice recognition. Iris scanners. The start of a new 007 movie, or how you access your bank accounts in 2017?

Recently, there has been widespread adoption of two-factor and multi-factor authentication. In addition to providing your username and password, you might have to provide something you have (such as a token) and prove who you are (fingerprint or voice).

Maybe with the exception of iris scanners, other biometric identification technologies have been quickly commercialized and scaled to consumer laptops, tablets, and smartphones, which can offer extra security and sometimes convenience. But, think for a moment about how you access the majority of your accounts—a list of usernames and passwords might come to mind.

You probably know you should use unique, complex passwords for each account. But, how do you remember them all? Do you write them on Post-It notes? Save them in Office documents*? Do you store those documents on a flash drive, your network or the cloud? What if any of those locations or devices were compromised?

Enter encrypted password managers. While no silver bullet (nothing in information security is), you can store and secure everything in a single program. You have your choice between online/cloud-based password managers and offline password managers. Many are cross-platform and keep your information synchronized across multiple devices.

Most password managers seamlessly integrate into your browser. Some password managers can integrate into select applications. If you're signing up for a new service, just about every password manager can even generate and store unique complex passwords for you.

Some password managers are free, and others aren't. You'll need to decide which one has the features and capabilities you need.

To get started, try the ones below. You can always start with a free version and migrate to a paid version if you want the extra features.

KeePass
KEEPASS.INFO

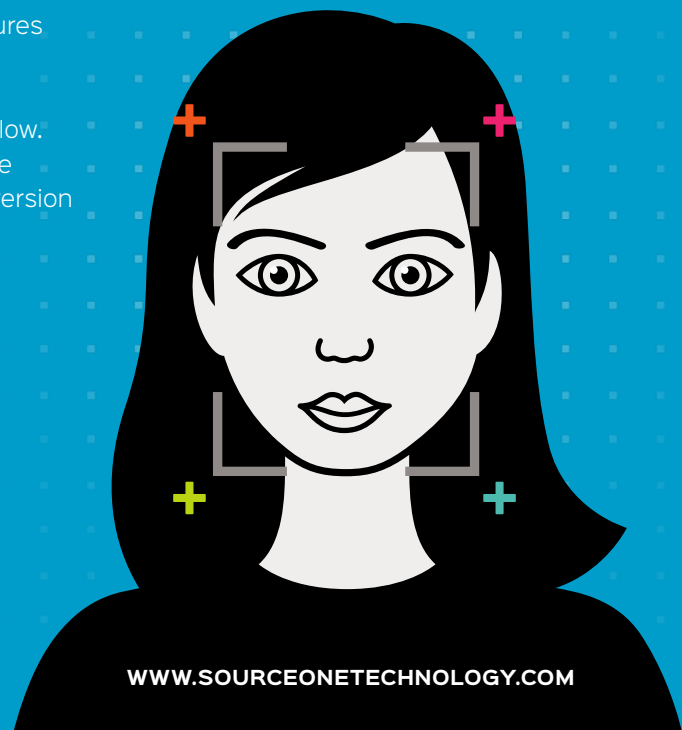
LastPass
LASTPASS.COM

1Password
1PASSWORD.COM

* Password-protected Excel/Word documents are better than nothing, but encryption in Office has been historically weak at best and can be quickly and easily cracked on today's hardware. Newer versions are implementing stronger encryption ciphers and protocols, but it's still recommended to avoid storing all of your usernames and passwords in Office documents.

Subscribe to 'The Source' and get all the latest issues straight to your inbox.

sourceonetechnology.com/the-source



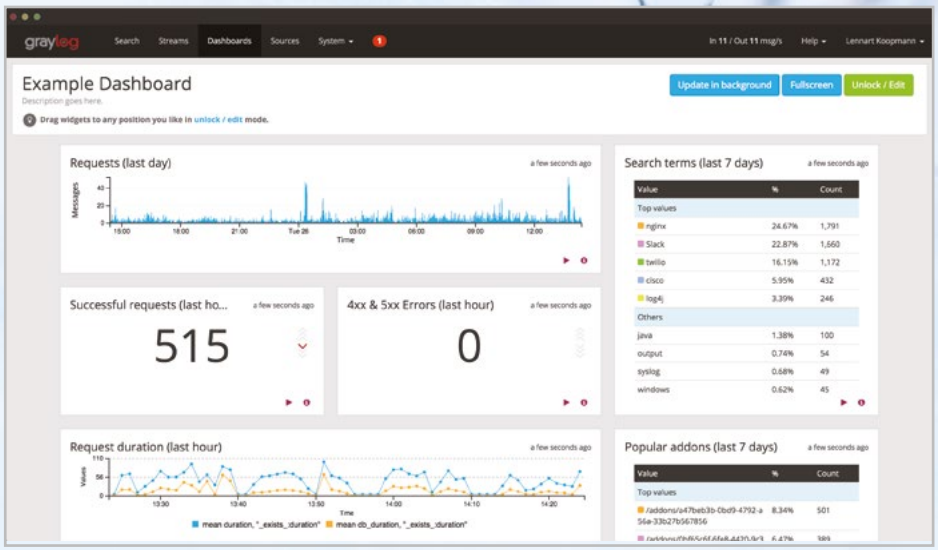
PACKETHUNTER

Our article on nextCloud in the last edition of The Source received a lot of attention, so we thought you'd love to hear about another great Open Source product we utilize in production environments - Graylog.

Over the past couple years, Source One Engineers have implemented Graylog servers within several of our client environments to keep an eye on crucial network activities. One primary use for us is monitoring Syslog messages that are generated from networking devices (such as firewall and switches) to determine if firmware bugs or physical hardware may be causing problems.

In more proactive scenarios, we like to use Graylog to send out alerts on key network infrastructure changes and logon attempts. For example, some of our clients would like to know when configuration changes are made to core switch configurations and when end-users VPN into their network.

You can setup custom trigger and alert filters to parse this information and setup how you would like to get notified.



A pre-built Graylog server can be imported into your virtual environment and be up and running collecting logging information within minutes.

Graylog is one of many Open Source products that makes our valuable software list.

You can find more information about Graylog and its many uses here:

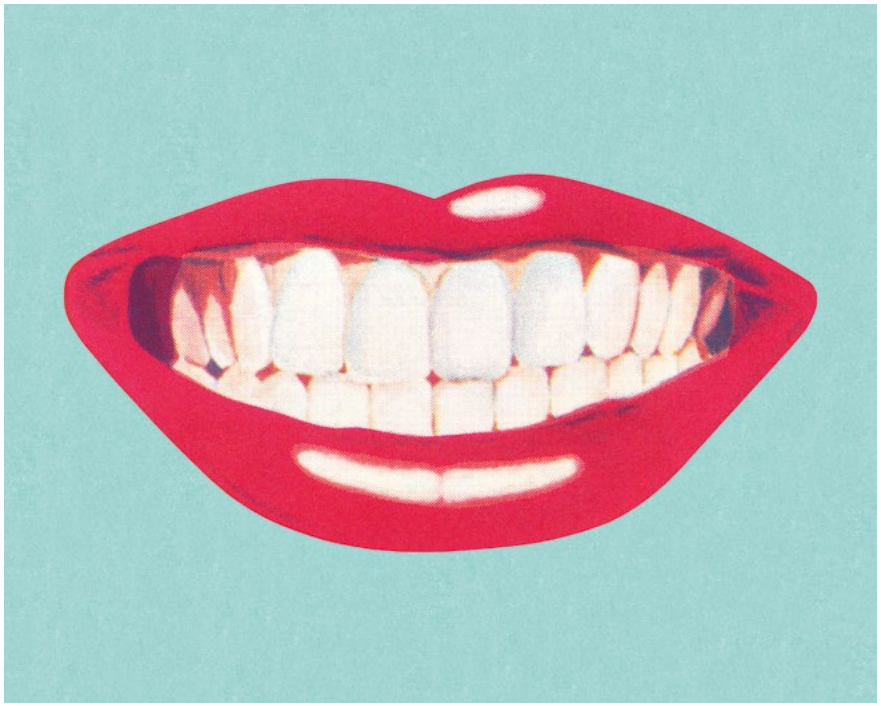
Website
GRAYLOG.ORG

Download
GRAYLOG.ORG/DOWNLOAD

Basic email hygiene

When it comes to basic email hygiene, prevention goes a long way. In fact, an old adage, which has become conventional wisdom over the years, states 'a closed relay keeps the spammers at bay'. OK, while that might be conventional wisdom, it's never been an old adage.

Whether you've inherited new infrastructure or have managed the same one for years, it's a good idea to periodically check your environment—specifically your mail server and firewall configurations—to ensure your organization doesn't unexpectedly wind up on any email or spam blacklists.



First, make sure you have outbound firewall rules in place which restrict port 25. The only system which should need this is your mail server, not your entire network. Anyone could start sending anonymous emails from your network whether they intend to—or not.

It's also pretty common for malware to leverage this port to continue spreading itself via email. Spam and malware being traced back to your organization? It's a surefire way to be blacklisted.

Second, ensure your mail server isn't configured as an open relay. Spammers constantly scan the Internet for open relays to route their email through, damaging your organization's email reputation in the process. It's another quick way to become blacklisted.

There are many other ways to protect your organization from becoming blacklisted, but these are some of the most common and basic quick checks you can do.

Check out our blog for more great tips, tricks, and guidance on managing your organization's email.

When you're done there, check out **www.mxtoolbox.com** for a great selection of additional tools and resources you can use to check and test various aspects of your email environment. You can even create a free account and have them monitor a few things for you!

"Look, Mom - no vulnerabilities!"

Calculating Disk IOPS

Have you ever wondered how many IOPS (Input/Output Operations per Second) your disk arrays are capable of producing?

Now you won't have to guess anymore! There's a highly effective IOPS calculator found online at **thecloudcalculator.com** that will help IT Administrators better understand the performance "capabilities" of any proposed array configuration based on the following:

- Disk type (SATA, SAS, SSD)
- Disk speed (7.2k, 10k, 15k, etc.)
- # of Physical disks
- RAID configuration (RAID 5, 6, 10)
- Expected read/write operation percentages

This tool may well change your opinion of how you previously configured disk arrays. After playing with various configuration choices available, you should begin to understand concepts such as:

- More physical disks in a logical array always equates to improved IOPS
- The higher the percentage of WRITE operations, the lower the performance (as compared to READ operations)
- If your application requires "x" IOPS, there are endless ways to achieve that goal – with various drive types, sizes, quantities, and RAID choice
- SSD easily outperforms older spindle-based disk technologies (at a huge financial cost)

Please also keep in mind, if your array is capable of delivering 3300 IOPS, but the applications/servers using that storage only consistently generate 400 IOPS (even under extremely HEAVY load), you've likely wasted a healthy portion of your IT budget on storage that could have been better allocated elsewhere.

So plan accordingly, and spend wisely!

What's the deal with the Windows 10 naming convention

At first, Windows was numbered. This included Windows 1.x, 2.x, and 3.x. Eventually, they moved on to years. These included: Windows 95 (released in 1995), Windows 98, 2000 and another favorite ME (Millennium Edition or another way to say 2000.)

Soon after that, Microsoft took an esoteric turn with Windows XP and Windows Vista. Finally, circling back to numbers: Windows 7, 8, 8.1, (no Windows 9) and Windows 10 – "The Last Version of Windows."* Easy enough, except the 4th version of Windows 10 is due in April of 2017.

Each of these versions may be is recognized by one of three names: Version Number, Name, and Codename. The final release of each also has a Kernal Version Number.

Release	Version #	Name	Codename	Kernal Version
1	1507	Original version	Threshold 1	10.0.10240
2	1511	November update	Threshold 2	10.0.10586
3	1607	Anniversary update	Redstone 1	10.0.14393
4	1704	Creator's update	Redstone 2	10.0.15025 (2/3/2017)

With Windows 10, Microsoft is trying to promote its prolific Operating Systems as SaaS - Software as a Service – i.e always under development and improvement. The path for Microsoft (or for that matter the IT industry) is continuously being planned, developed and implemented. So, until the next greatest thing comes along, enjoy Windows 10... whichever version you are running.

* theverge.com/2015/5/7/8568473/windows-10-last-version-of-windows.

LOVE FREE?

If you like getting impartial advice, practical tips, and pointers to great free software, then we've got even more for you!

CONNECT

Read the latest from our engineers or ask us a question whenever you need advice.


sourceonetechnology.com/blog


@sourceone_wi


linkedin.com/company/source-one-technology-inc

Out of all the IT companies we evaluated both in Milwaukee and our corporate headquarters in Washington DC, Source One Technology is the only company that understands how to build a solid IT infrastructure from top to bottom.

Waleed Gamay
VP OF OPERATIONS
DREAMPAK, LLC - NEW BERLIN

See what our customers are saying about us
sourceonetechnology.com/testimonials

Source One TECHNOLOGY

To find out how we can help you save time and money on frustrating network and computer issues, call (262) 993 2231 or visit www.sourceonetechnology.com.