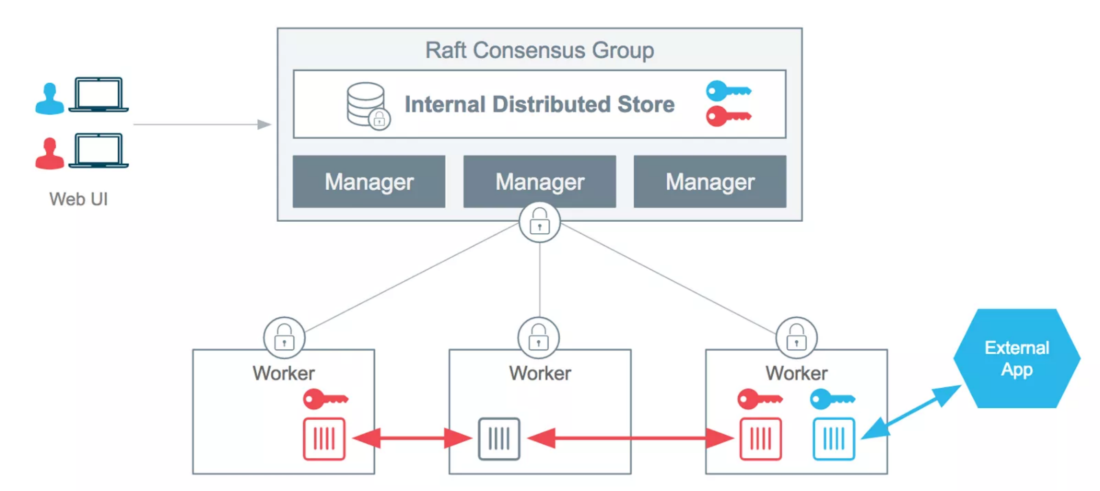
Security Newsletter

17 February 2017

Docker introduces Secret



We fundamentally believe that apps are safer if there is a standardized interface for accessing secrets. Any good solution will also have to follow security best practices, such as encrypting secrets while in transit; encrypting secrets at rest; preventing secrets from unintentionally leaking when consumed by the final application; and strictly adhere to the principle of least-privilege, where an application only has access to the secrets that it needs—no more, no less.

By integrating secrets into Docker orchestration, we are able to deliver a solution for the secrets management problem that follows these exact principles.

Read More

AWS Announces CISPE Membership and Compliance with First-Ever Code of Conduct for Data Protection in the Cloud

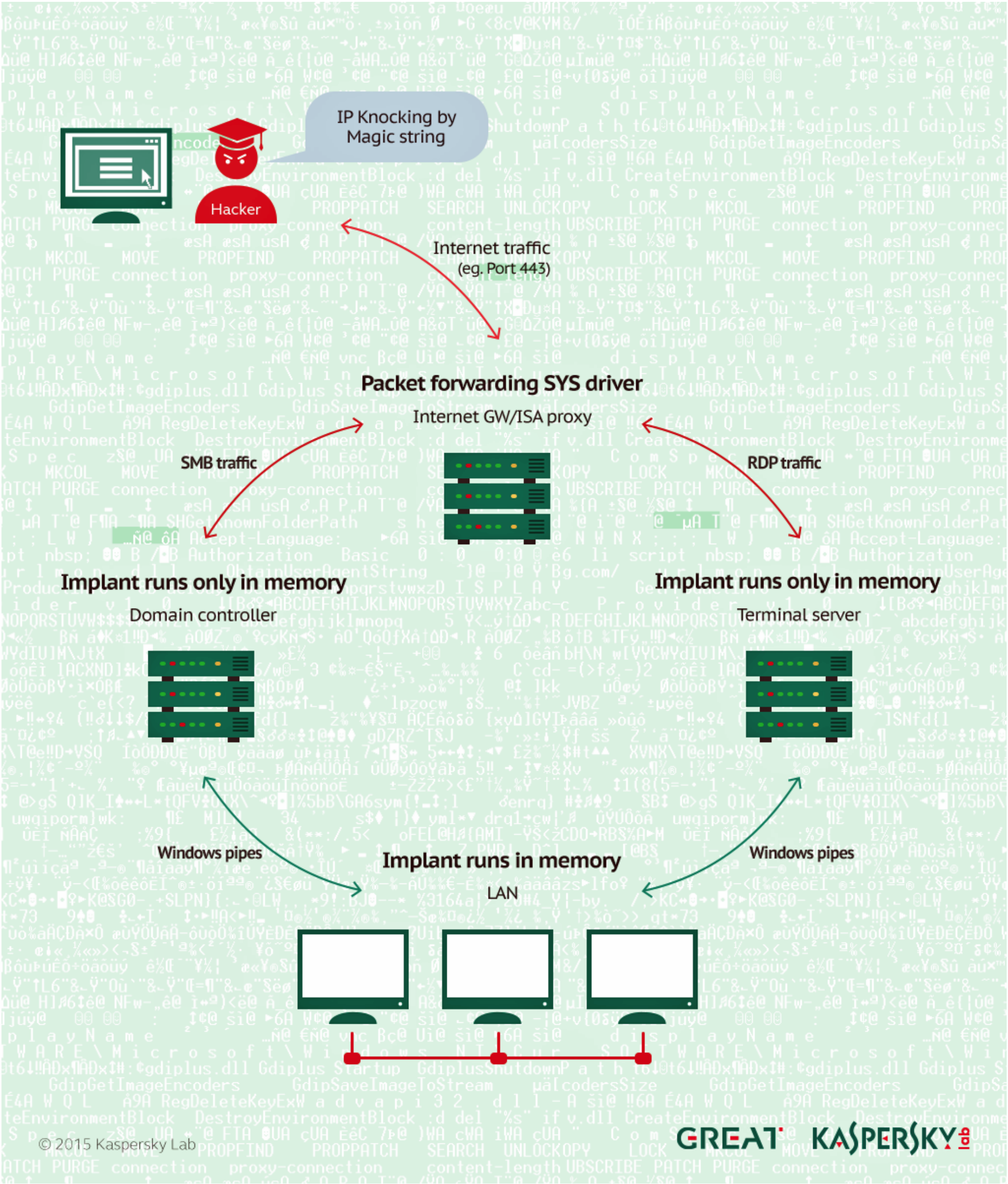
CLOUD WITH CONFIDENCE
CISPE – Cloud Infrastructure Services Providers in Europe – is the trade association that gives a voice to cloud infrastructure providers at European level.
CISPE Code of Conduct

In order to show AWS's continued commitment to ensuring that customers can comply with EU Data Protection requirements when using our services. Amazon announced they joined the CISPE (Cloud Infrastructure Services Providers in Europe) and announced compliance with their code of conduct on several services they offer through AWS.

Please note that it does not include all AWS services yet: EC2 (servers), S3 (file storage), RDS (databases), IAM (Access management), Cloudtrail (logging) and EBS (storage space "for rapidly moving "dynamic" data such as operating system files, databases, etc) are in the scope for now.

Read More

A rash of invisible, fileless malware is infecting banks around the globe



Fileless malware is going mainstream, as financially motivated criminal hackers mimic their nation-sponsored counterparts. Those malwares evade detection by reducing or eliminating the storage of any binaries on disk and instead hides its code in the registry of a compromised host

The researchers don't yet know how the malware initially takes hold. Possible vectors include SQL-injection attacks and exploits targeting plugins for the WordPress content management application. This is a good reminder that Antivirus is not a silver bullet that can anihilate any threats. It is important for IT administrators, developers and end users stay aware of the risks and act responsibily.

Read More

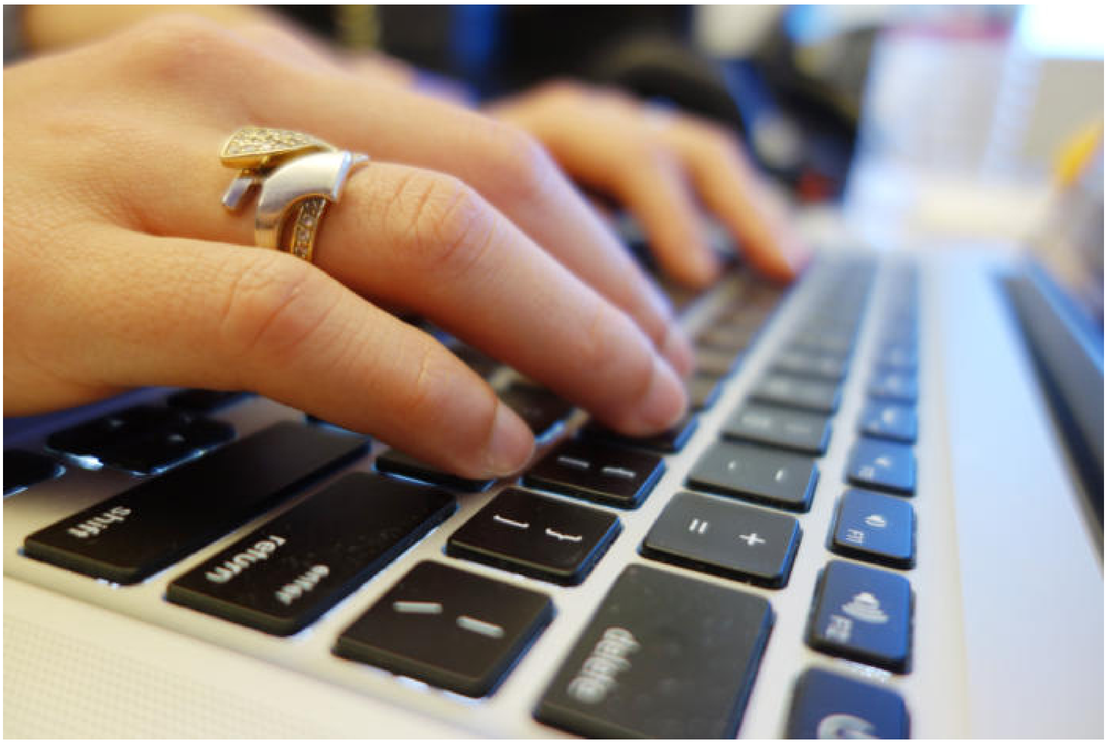
Everything you need to know about HTTP security headers

What can be attacked must be defended, and since tradition requires all security features to be a bolted-on afterthought, things… got a little complicated.

This article explains what secure headers are and how to implement these headers in Rails, Django, Express.js, Go, Nginx, and Apache.

Read More

Phishing: Malware distributors are switching to less suspicious file types

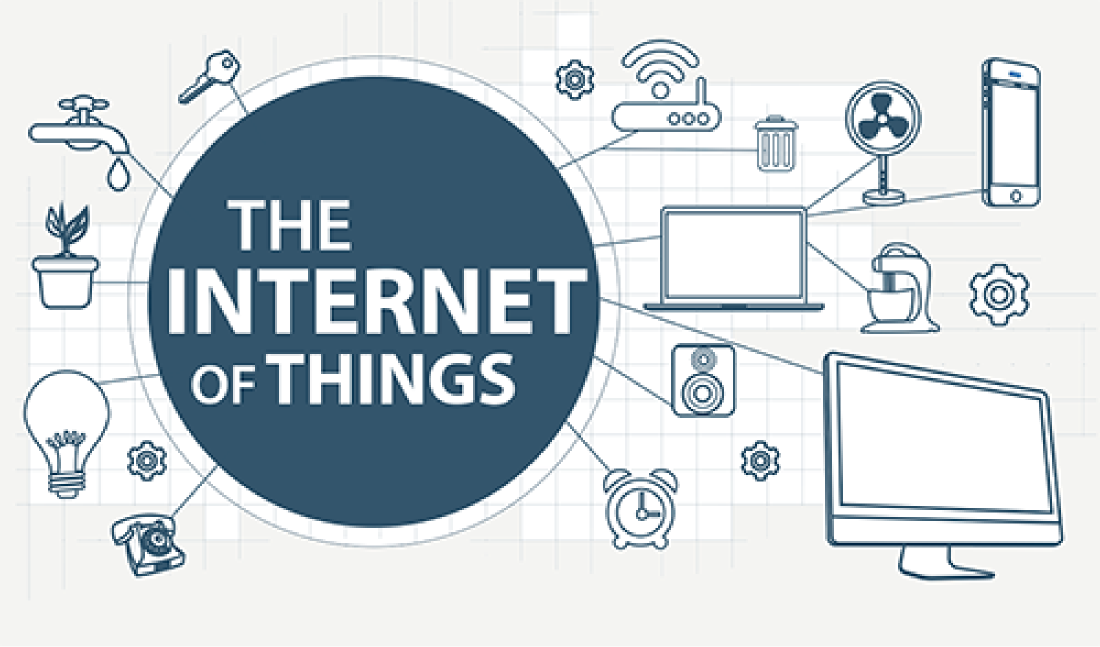


After aggressively using JavaScript email attachments to distribute malware for the past year, attackers are now switching to less suspicious file types to trick users. Last week, researchers from the Microsoft Malware Protection Center warned about a new wave of spam emails that carried malicious .LNK files inside ZIP archives. Those files had malicious PowerShell scripts attached to them.

In the recent campaign seen by Microsoft, the malicious LNK files contained a PowerShell script that downloaded and installed the Kovter click fraud trojan. Another file type used to distribute malware in recent months has been SVG (Scalable Vector Graphics). While many people correctly associate .SVG files with images, it's a little-known fact that such files can actually contain JavaScript.

Read More

Security and Privacy Guidelines for the Internet of Things



Lately, Bruce Schneier, a well-known cybersecurity expert, has been collecting IoT security and privacy guidelines. He posted everything he has found on the subject on his blog.

They all largely say the same things: avoid known vulnerabilities, don't have insecure defaults, make your systems patchable, and so on. He is guessing that regulation on the subject is coming soon and vendors must get ready for their upcoming products.

Read More

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.