SOPHOS

SIGNATURE SYSTEMS, INC
PDQ
TECHNOLOGY SERVICES

Ransomware today:
How to protect against Locky and friends

What we’re going to cover

- Anatomy of a ransomware attack
- The latest ransomware to rear its ugly head – introducing Locky and its friends
- Why these attacks are so successful
- Practical steps to protect your organization from ransomware threats
- How Sophos can help

A bit of background

Ransomware is a form of malware that encrypts private information and demands payment in order to decrypt it.

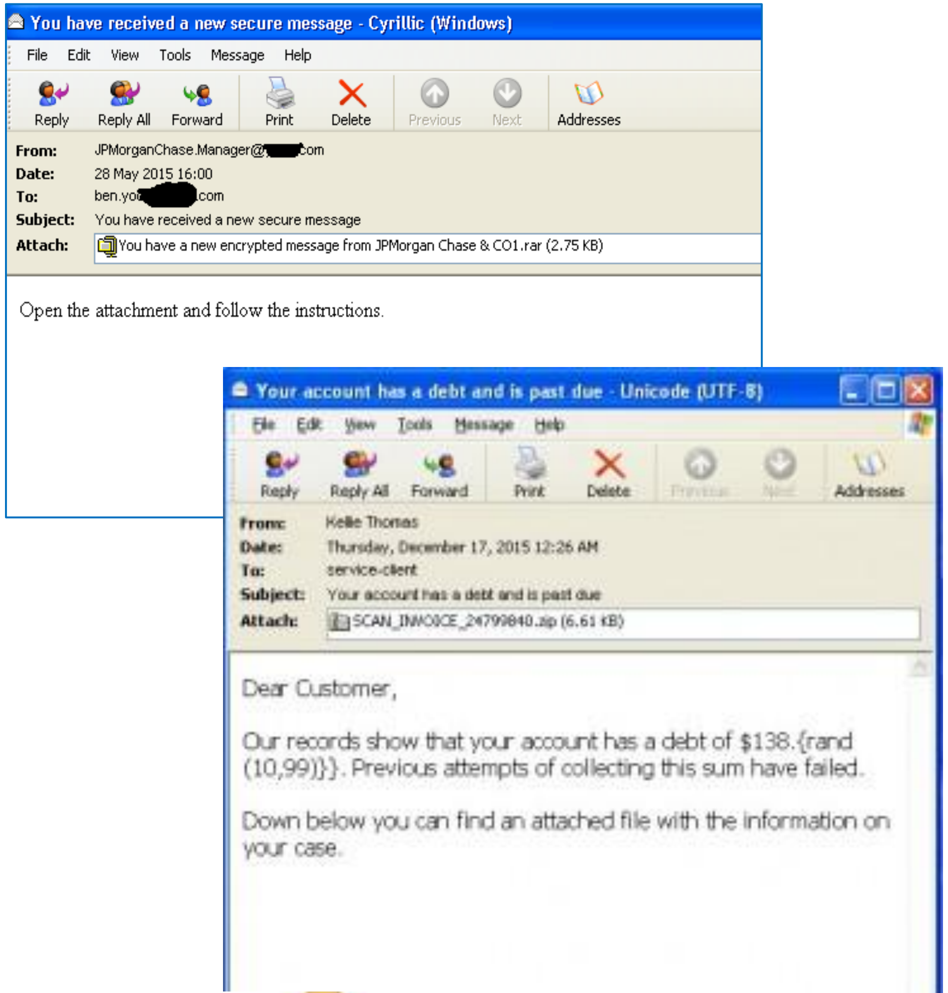
History

- CryptoLocker first appeared in 2013
- New variants emerge all-too-regularly
- Current wave has roots in the early days of FakeAV
- Locky is one of the newest flavors to menace internet users
- Common ransom demands for USD 200 – 500.
- Technology used changes rapidly
  - Office documents with macros
  - CHM files
  - JavaScript
  - .bat files

2 main vectors of attack

- **SPAM** (via social engineering)
  - Seemingly plausible sender
  - Has attachment e.g. invoice, parcel delivery note
  - The attachment contains an embedded macro
  - When the attachment is opened the macro downloads and then executes the ransomware payload
  - Used by Locky, TorrentLocker, CTB-Locker

- **Exploit kits**
  - Black market tools used to easily create attacks that exploit known or unknown vulnerabilities (zero-day)
  - Client side vulnerabilities usually target the Web browser
  - Used by Angler, CryptoWall, TeslaCrypt, CrypVault, ThreatFinder



From: JPMorganChase.Manager@[redacted]com
Date: 28 May 2015 16:00
To: ben.yo[redacted]com
Subject: You have received a new secure message
Attach: You have a new encrypted message from JPMorgan Chase & CO1.rar (2.75 KB)

Open the attachment and follow the instructions.

From: Kellie Thomas
Date: Thursday, December 17, 2015 12:26 AM
To: service-client
Subject: Your account has a debt and is past due
Attach: SCAN_INVOICE_24799840.zip (6.61 KB)

Dear Customer,

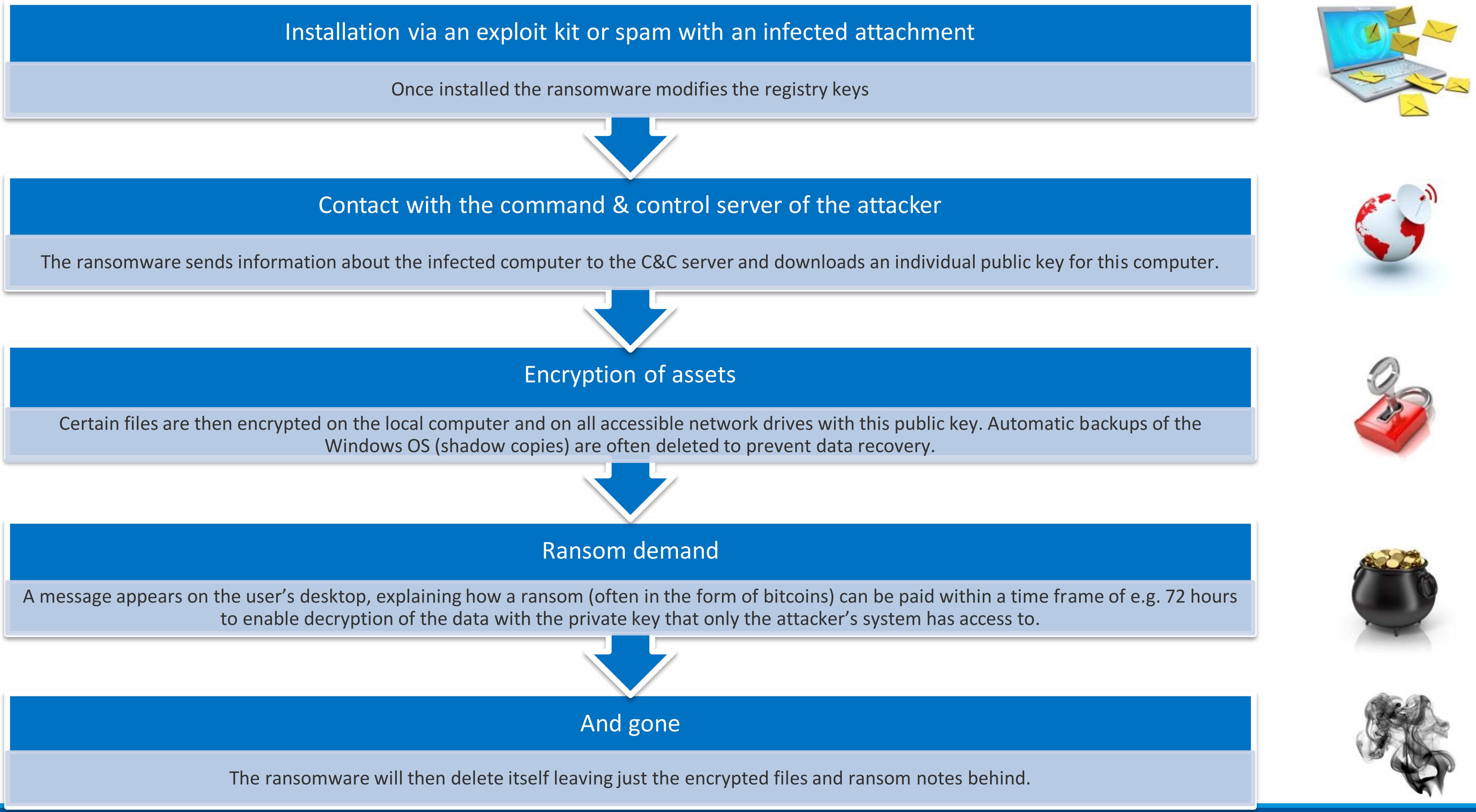
Our records show that your account has a debt of $138.{rand (10,99)}. Previous attempts of collecting this sum have failed.

Down below you can find an attached file with the information on your case.

SOPHOS

Anatomy of a ransomware attack

Anatomy of a ransomware attack



Installation via an exploit kit or spam with an infected attachment

Once installed the ransomware modifies the registry keys

Contact with the command & control server of the attacker

The ransomware sends information about the infected computer to the C&C server and downloads an individual public key for this computer.

Encryption of assets

Certain files are then encrypted on the local computer and on all accessible network drives with this public key. Automatic backups of the Windows OS (shadow copies) are often deleted to prevent data recovery.

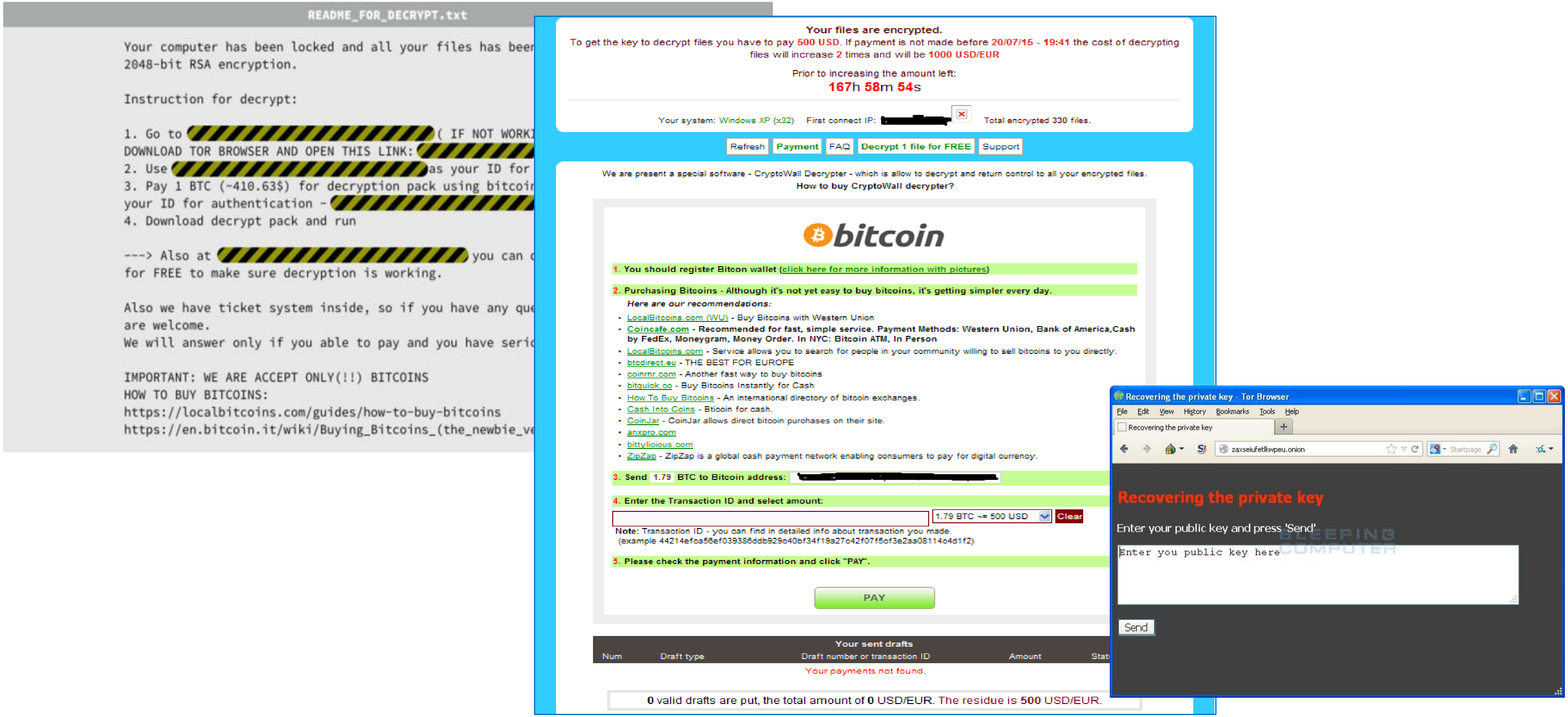
Ransom demand

A message appears on the user’s desktop, explaining how a ransom (often in the form of bitcoins) can be paid within a time frame of e.g. 72 hours to enable decryption of the data with the private key that only the attacker’s system has access to.

And gone

The ransomware will then delete itself leaving just the encrypted files and ransom notes behind.

Ransom demands



README_FOR_DECRYPT.txt

```
Your computer has been locked and all your files has been
2048-bit RSA encryption.

Instruction for decrypt:

1. Go to [redacted] ( IF NOT WORKI
DOWNLOAD TOR BROWSER AND OPEN THIS LINK: [redacted]
2. Use [redacted] as your ID for
3. Pay 1 BTC (~410.63$) for decryption pack using bitcoi
your ID for authentication - [redacted]
4. Download decrypt pack and run

---> Also at [redacted] you can d
for FREE to make sure decryption is working.

Also we have ticket system inside, so if you have any que
are welcome.
We will answer only if you able to pay and you have seri

IMPORTANT: WE ARE ACCEPT ONLY(!!) BITCOINS
HOW TO BUY BITCOINS:
https://localbitcoins.com/guides/how-to-buy-bitcoins
https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_ve
```

Your files are encrypted.

To get the key to decrypt files you have to pay 500 USD. If payment is not made before 20/07/15 - 19:41 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR

Prior to increasing the amount left:

167h 58m 54s

Your system: Windows XP (x32) First connect IP: [redacted] Total encrypted 330 files.

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You should register Bitcon wallet (click here for more information with pictures)
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

   Here are our recommendations:

   - LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
   - Coincafe.com - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
   - LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
   - btcdirect.eu - THE BEST FOR EUROPE
   - coinrnr.com - Another fast way to buy bitcoins
   - bitquick.co - Buy Bitcoins Instantly for Cash
   - How To Buy Bitcoins - An international directory of bitcoin exchanges.
   - Cash Into Coins - Bticoin for cash.
   - CoinJar - CoinJar allows direct bitcoin purchases on their site.
   - anxpro.com
   - bittylicious.com
   - ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
3. Send 1.79 BTC to Bitcoin address: [redacted]
4. Enter the Transaction ID and select amount:

   1.79 BTC ~= 500 USD Clear

   Note: Transaction ID - you can find in detailed info about transaction you made.
   (example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)
5. Please check the payment information and click "PAY".

Your sent drafts

Num	Draft type	Draft number or transaction ID	Amount	Stat

Your payments not found.

0 valid drafts are put, the total amount of 0 USD/EUR. The residue is 500 USD/EUR.

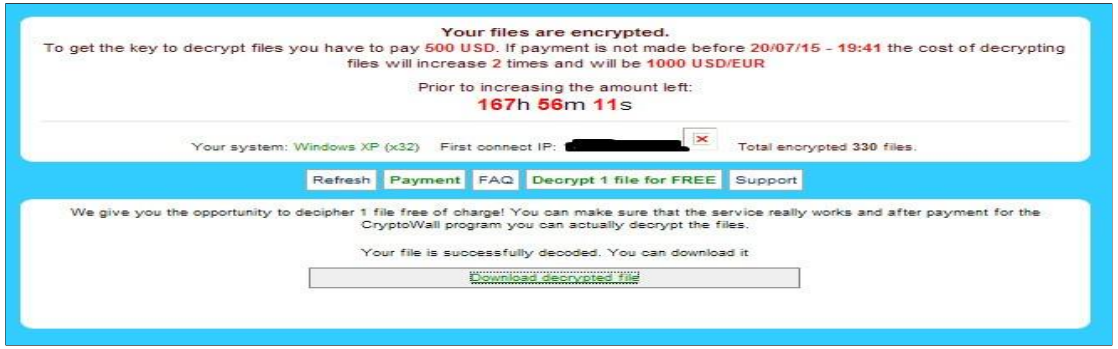
Recovering the private key

Enter your public key and press 'Send'

Enter you public key here

Paying ransoms

- Payment is made in Bitcoins
- Instructions are available via Tor
- The ransom increases the longer you take to pay
- On payment of the ransom, the public encryption key is provided so you can decrypt your computer files



Your files are encrypted.

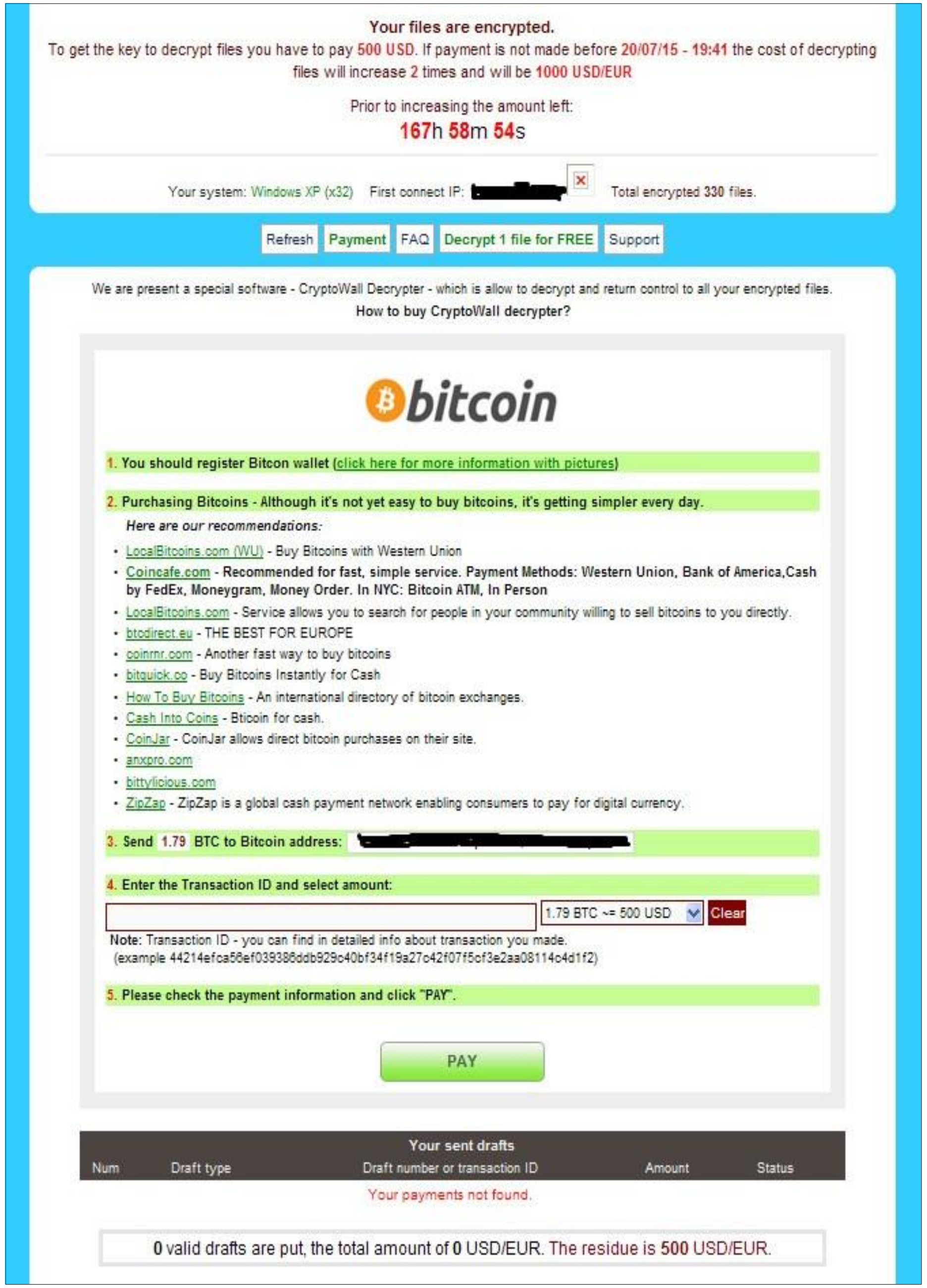
To get the key to decrypt files you have to pay 500 USD. If payment is not made before 20/07/15 - 19:41 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR

Prior to increasing the amount left:
167h 56m 11s

Your system: Windows XP (x32) First connect IP: [redacted] Total encrypted 330 files.

We give you the opportunity to decipher 1 file free of charge! You can make sure that the service really works and after payment for the CryptoWall program you can actually decrypt the files.

Your file is successfully decoded. You can download it



Your files are encrypted.

To get the key to decrypt files you have to pay 500 USD. If payment is not made before 20/07/15 - 19:41 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR

Prior to increasing the amount left:
167h 58m 54s

Your system: Windows XP (x32) First connect IP: [redacted] Total encrypted 330 files.

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You should register Bitcon wallet (click here for more information with pictures)
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

   Here are our recommendations:

   - LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
   - Coincafe.com - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
   - LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
   - btcdirect.eu - THE BEST FOR EUROPE
   - coinrnr.com - Another fast way to buy bitcoins
   - bitquick.co - Buy Bitcoins Instantly for Cash
   - How To Buy Bitcoins - An international directory of bitcoin exchanges.
   - Cash Into Coins - Bticoin for cash.
   - CoinJar - CoinJar allows direct bitcoin purchases on their site.
   - anxpro.com
   - bittylicious.com
   - ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
3. Send 1.79 BTC to Bitcoin address: [redacted]
4. Enter the Transaction ID and select amount:

   1.79 BTC ~= 500 USD

   Note: Transaction ID - you can find in detailed info about transaction you made.
   (example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)
5. Please check the payment information and click "PAY".

Your sent drafts

Num	Draft type	Draft number or transaction ID	Amount	Status

Your payments not found.

0 valid drafts are put, the total amount of 0 USD/EUR. The residue is 500 USD/EUR.

SOPHOS

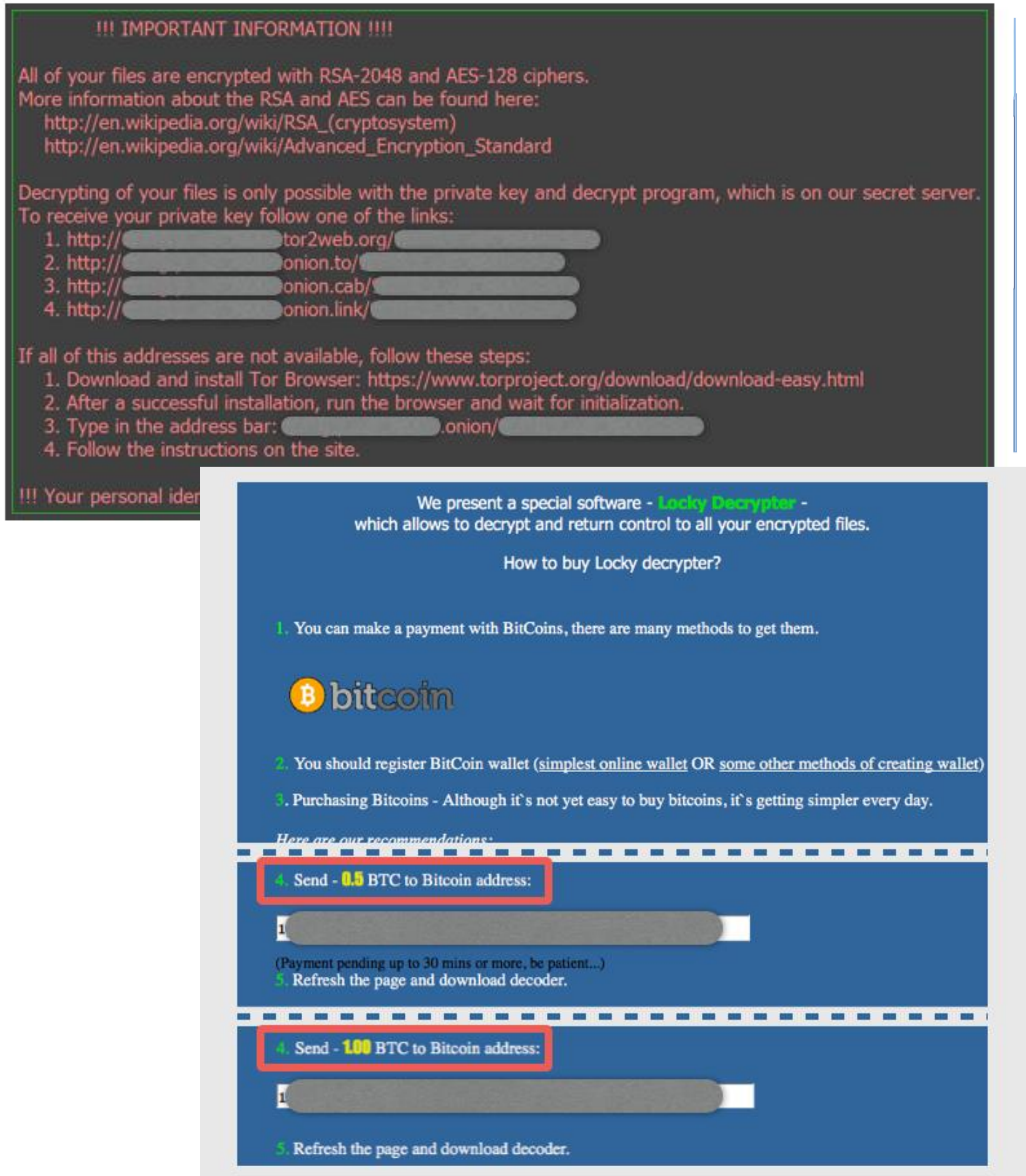
Common ransomware: Locky and friends

Locky: the new kid on the block

- Nickname of a new strain of ransomware, so-called because it renames all your important files so that they have the extension .locky
- Ransoms vary from BTC 0.5 to BTC 1.00 (1 BTC is worth about $400/£280).
- Started hitting the headlines in early 2016
- Wreaking havoc with at least 400,000 machines affected worldwide

A common Locky attack

- You receive an email containing an attached document.
  - The document looks like gobbledegook.
  - The document advises you to enable macros "if the data encoding is incorrect."
  - The criminals want you to click on the 'Options' button at the top of the page.
- Once you click Options, Locky will start to execute on your computer.
- As soon as it is ready to ask you for the ransom, it changes your desktop wallpaper.
- The format of the demand varies, but the results are the same.



!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://[redacted]tor2web.org/[redacted]
2. http://[redacted]onion.to/[redacted]
3. http://[redacted]onion.cab/[redacted]
4. http://[redacted]onion.link/[redacted]

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [redacted].onion/[redacted]
4. Follow the instructions on the site.

!!! Your personal ider

We present a special software - Locky Decrypter -
which allows to decrypt and return control to all your encrypted files.

How to buy Locky decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.

2. You should register BitCoin wallet (simplest online wallet OR some other methods of creating wallet)

3. Purchasing Bitcoins - Although it`s not yet easy to buy bitcoins, it`s getting simpler every day.

Here are our recommendations:

4. Send - 0.5 BTC to Bitcoin address:

1[redacted]

(Payment pending up to 30 mins or more, be patient...)
5. Refresh the page and download decoder.

4. Send - 1.00 BTC to Bitcoin address:

1[redacted]

5. Refresh the page and download decoder.

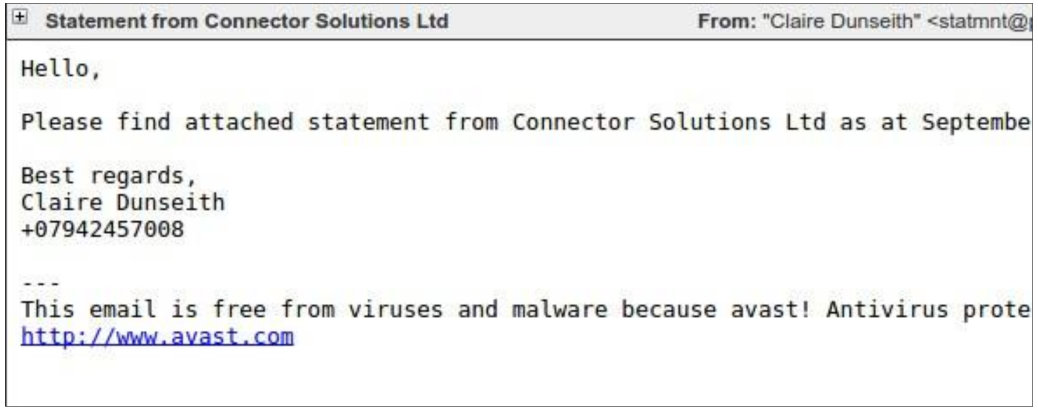
Different ransom demands by "Locky" at different times

TorrentLocker

- Almost exclusively distributed via sophisticated spam campaigns
  - High quality emails
  - Translated into multiple languages (Dutch, Japanese, Korean, Italian, Spanish …)
- Highly targeted geographically
- **Peculiarity:** Use of the victim machine’s address book to send the ransomware to other machines
- Communicates with its C&C server in HTTPS (POST requests) to make detection more difficult

CTB-Locker

- **Peculiarity:** Business model based on affiliations
  - Infections are conducted by 'partners' who receive in return a portion of the takings
  - Enables faster spreading of malicious code
  - Approach notably used in the past by Fake-AV
- The cyber crooks offer the option of a monthly payment
- Has also been widely distributed by the Rig and Nuclear exploit kits
- As with TorrentLocker, the majority of infections have started via spam campaigns



Statement from Connector Solutions Ltd **From:** "Claire Dunseith" <statmnt@

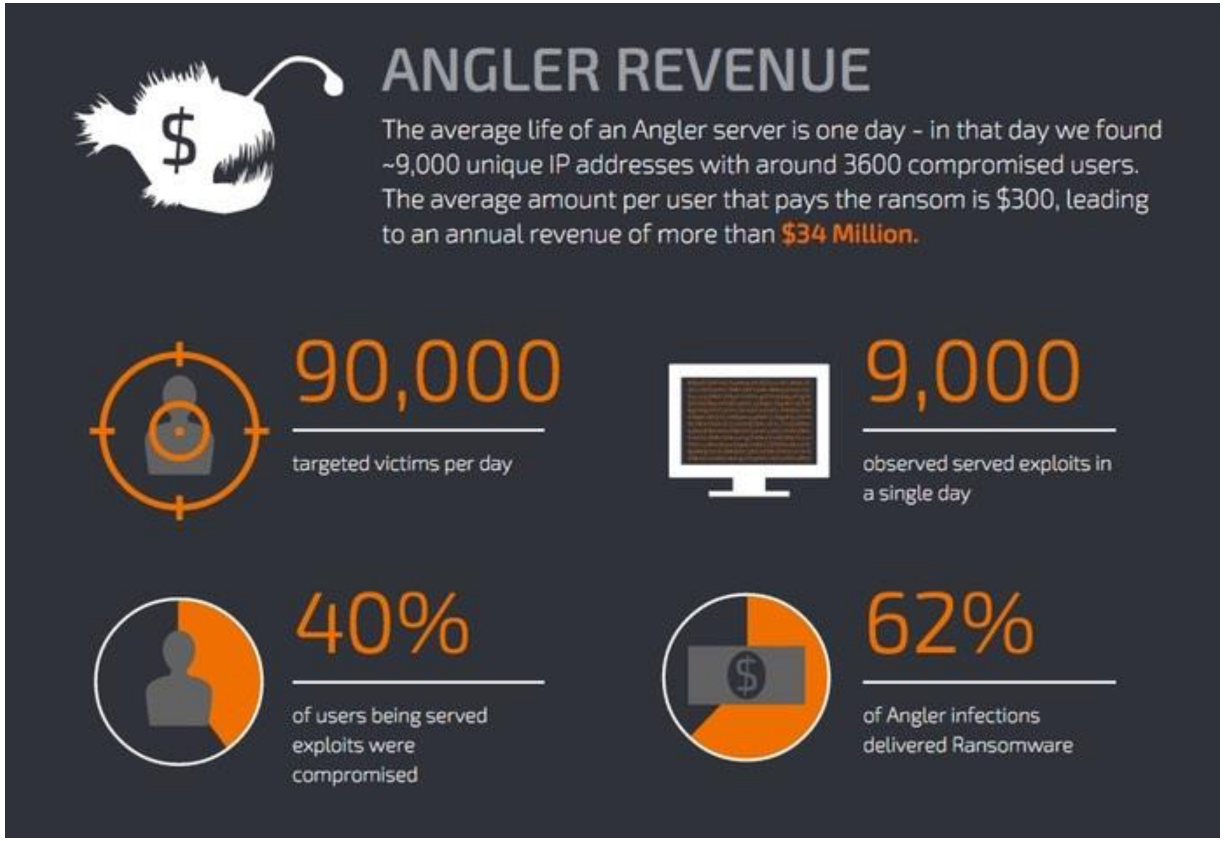
```
Hello,

Please find attached statement from Connector Solutions Ltd as at Septembe

Best regards,
Claire Dunseith
+07942457008

---
This email is free from viruses and malware because avast! Antivirus prote
http://www.avast.com
```

CTB-Locker variant that attacks websites

- Same name as the ransomware that attacks Windows computers
- Written in PHP
- First attack in the UK on 12th February 2016
- Already many hundreds of sites have been attacked
- Attacks websites by encrypting all files in their repositories
- A password-protected ‘shell’ is installed on most of the affected sites, allowing attackers to connect to the server(s) via a backdoor

Angler: an all-too-well-known exploit kit

- Grown in notoriety since mid 2014
  - The payload is stored in memory and the disk file is deleted
  - Detects security products and virtual machines
  - Ability to spread many infections: banking Trojans, backdoor, rootkits, ransomware
- Easy to use
  - Doesn’t require any particular technical competence
  - Available for a few thousand USD on the Dark Web



ANGLER REVENUE

The average life of an Angler server is one day - in that day we found ~9,000 unique IP addresses with around 3600 compromised users. The average amount per user that pays the ransom is $300, leading to an annual revenue of more than $34 Million.

90,000 targeted victims per day

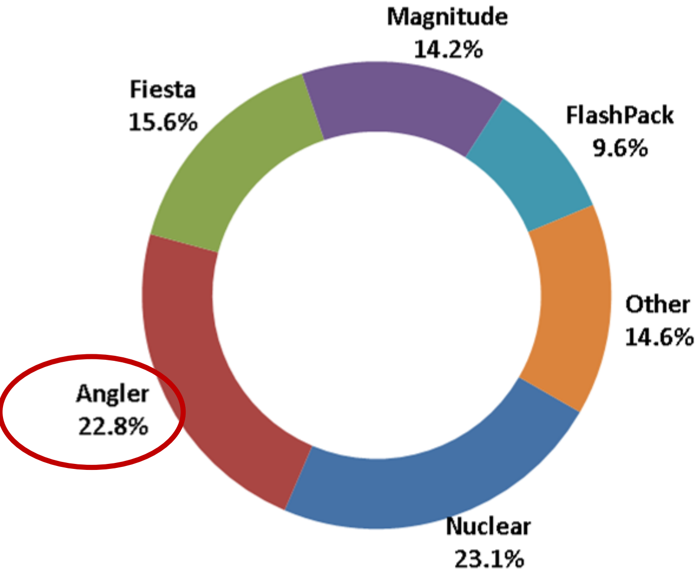
9,000 observed served exploits in a single day

40% of users being served exploits were compromised

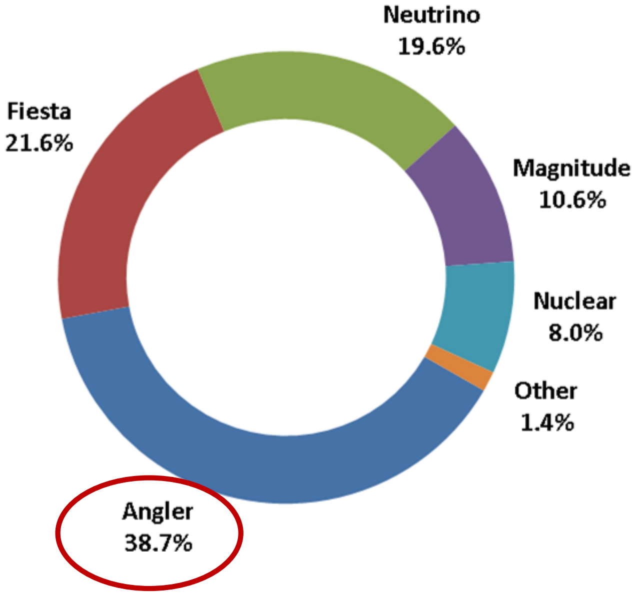
62% of Angler infections delivered Ransomware

Angler’s evolution into the dominant exploit kit

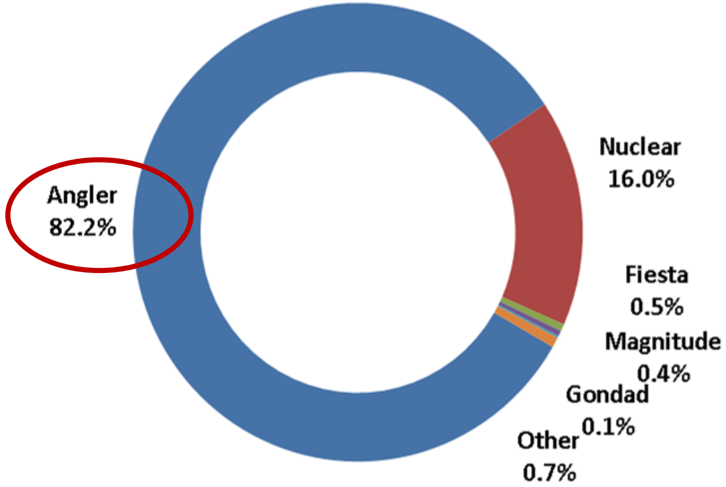
Sep 2014



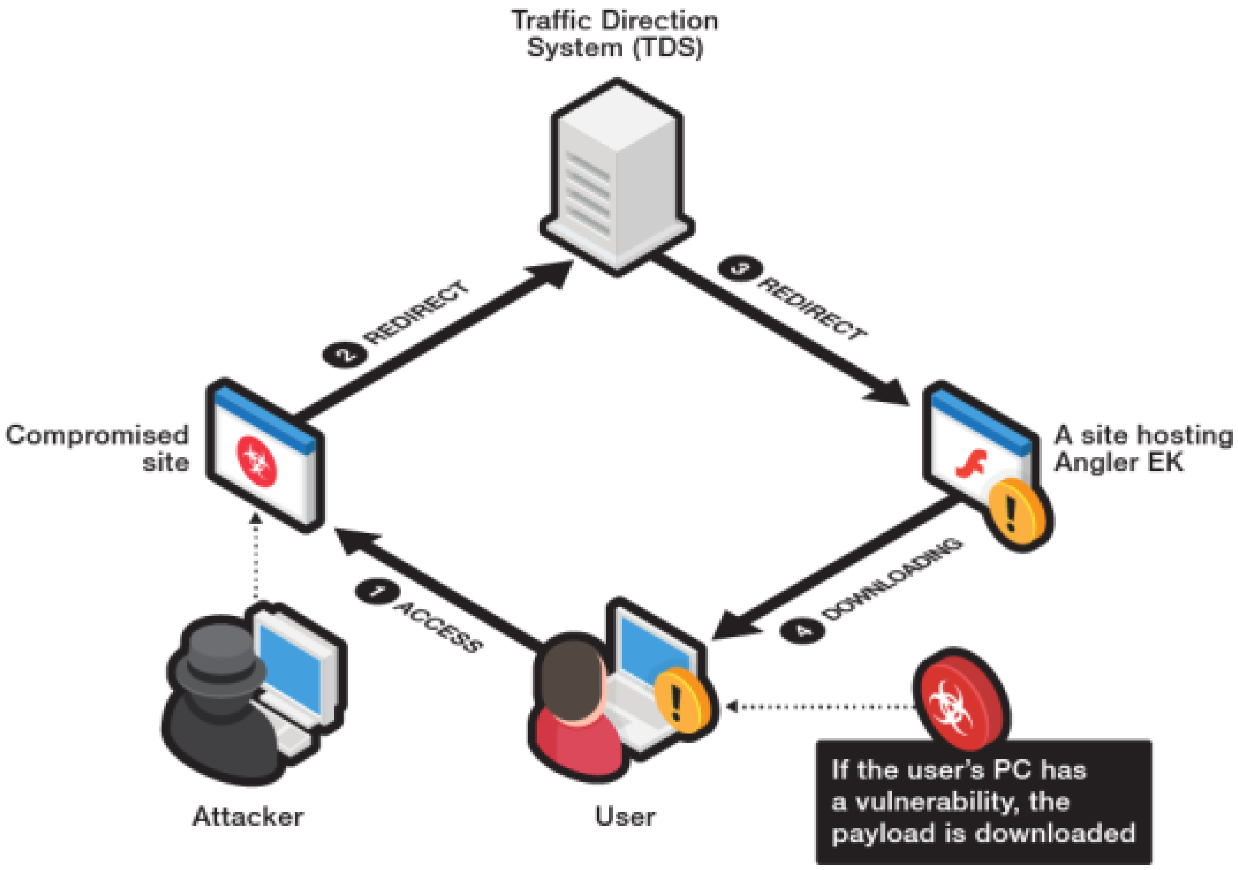
Jan 2015



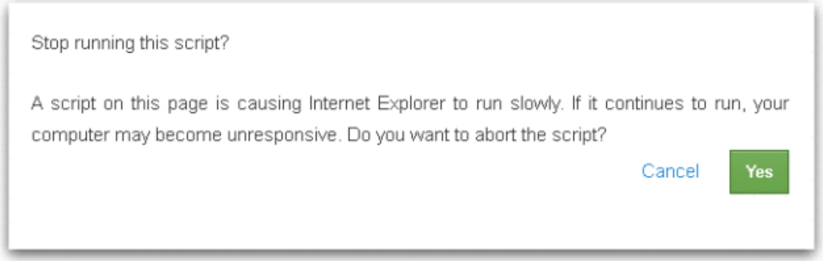
May 2015



Chain of infection for Angler exploit kits


Traffic Direction System (TDS)
2 REDIRECT
3 REDIRECT
Compromised site
A site hosting Angler EK
1 ACCESS
4 DOWNLOADING
Attacker
User
If the user's PC has a vulnerability, the payload is downloaded

1. The victim accesses a compromised web server through a vulnerable browser
2. The compromised web server redirects the connection to an intermediary server
3. In turn, the intermediary server redirects the connection to the attacker’s server which hosts the destination page of the exploit kit
4. The destination page looks for vulnerable plug-ins (Java, Flash, Silverlight) and their version numbers
5. If a vulnerable browser or plug in is detected the exploit kit releases its payload and infects the system.


Stop running this script?

A script on this page is causing Internet Explorer to run slowly. If it continues to run, your computer may become unresponsive. Do you want to abort the script?

SOPHOS

Why these attacks are so successful

Why are these attacks so successful?

Professional attack technology

- Highly professional approach e.g. usually provides the actual decryption key after payment of the ransom
- Skillful social engineering
- Hide malicious code in technologies that are permitted in many companies e.g. Microsoft Office macros, JavaScript, VBScript, Flash …

Why are these attacks so successful?

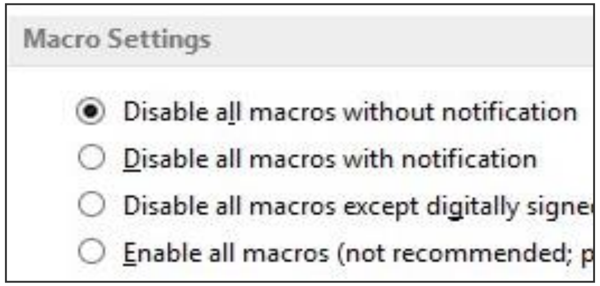
Security weaknesses in the affected companies

- Inadequate backup strategy
- Updates and patches are not implemented swiftly enough
- Dangerous user/ rights permissions – more than they need
- Lack of user security training
- Security systems are not implemented or used correctly
- Lack of IT security knowledge
- Conflicting priorities: security vs productivity concerns

Practical steps to protect against ransomware

Best practices – do this NOW!

1. Backup regularly and keep a recent backup copy off-site.
2. Don’t enable macros in document attachments received via email.
3. Be cautious about unsolicited attachments.
4. Don’t give yourself more login power than you need.
5. Consider installing the Microsoft Office viewers.
6. Patch early, patch often.
7. Configure your security products correctly.



Macro Settings

● Disable all macros without notification
○ Disable all macros with notification
○ Disable all macros except digitally signe
○ Enable all macros (not recommended; p

Security solution requirements

As a minimum you should:

- Deploy antivirus protection
- Block spam
- Use a sandboxing solution
- Block risky file extensions (javascript, vbscript, chm etc…)
- Password protect archive files
- Use URL filtering (block access to C&C servers)
- Use HTTPS filtering
- Use HIPS (host intrusion prevention service)
- Activate your client firewalls
- Use a whitelisting solution

Additional steps

- Employee awareness & training
  - Sophos IT Security Dos and Don’ts
  - Sophos Threatsaurus
- Segment the company network
  - NAC solutions ensure only known computers can access the network
  - Separate functional areas within a firewall e.g. client and server networks
- Encrypt company data
  - It doesn’t stop the ransomware but prevents damage caused by sensitive documents getting into the wrong hands
- Use security analysis tools
  - If an infection does occur, it’s vital that the source is identified and contained ASAP.

Threatsaurus

The A-Z of computer and data security threats

SOPHOS

In collaboration with the Center for Internet Security

How Sophos can help

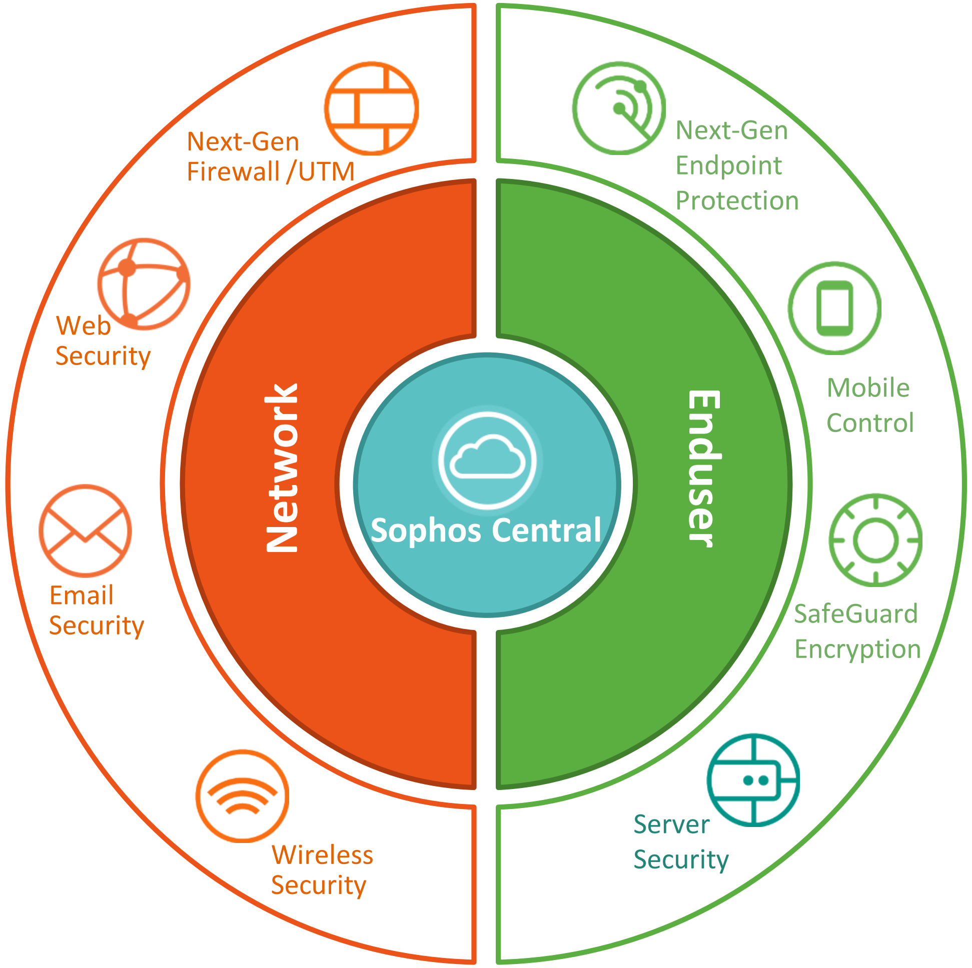
Compete protection: Enduser and Network

Secure the Perimeter
Ultimate enterprise firewall performance, security, and control.

Secure the Web
Advanced protection, control, and insights that's effective, affordable, and easy.

Secure the Email
Email threats and phishing attacks don't stand a chance.

Secure the Wireless
Simple, secure Wi-Fi connection.



Secure the Endpoint (PC/Mac)
Next Gen Endpoint security to prevent, detect, investigate and remediate

Secure the Mobile Device
Secure smartphones and tablets just like any other endpoint

Protect the Data
Simple-to-use encryption for a highly effective last line of defense against data loss

Secure the Servers
Protection optimized for server environment (physical or virtual): fast, effective, controlled

Security as a System

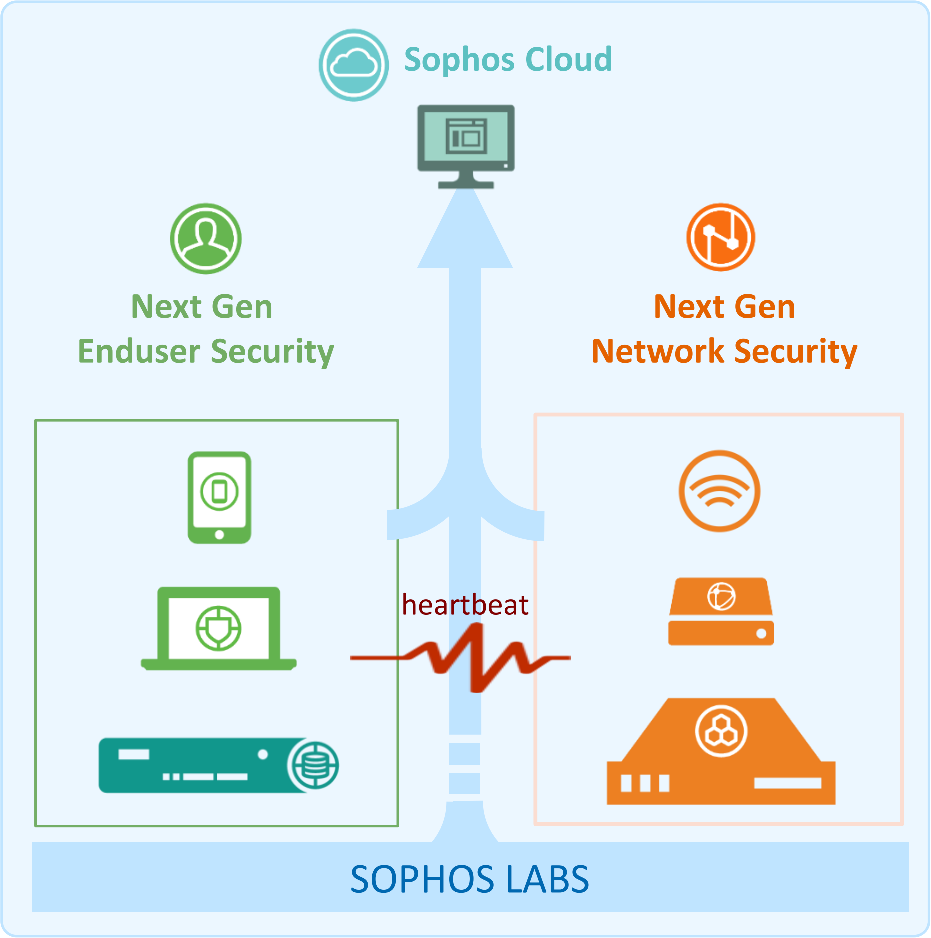
Security must be comprehensive
The capabilities required to fully satisfy customer need

Security is more effective as a system
New possibilities through technology cooperation

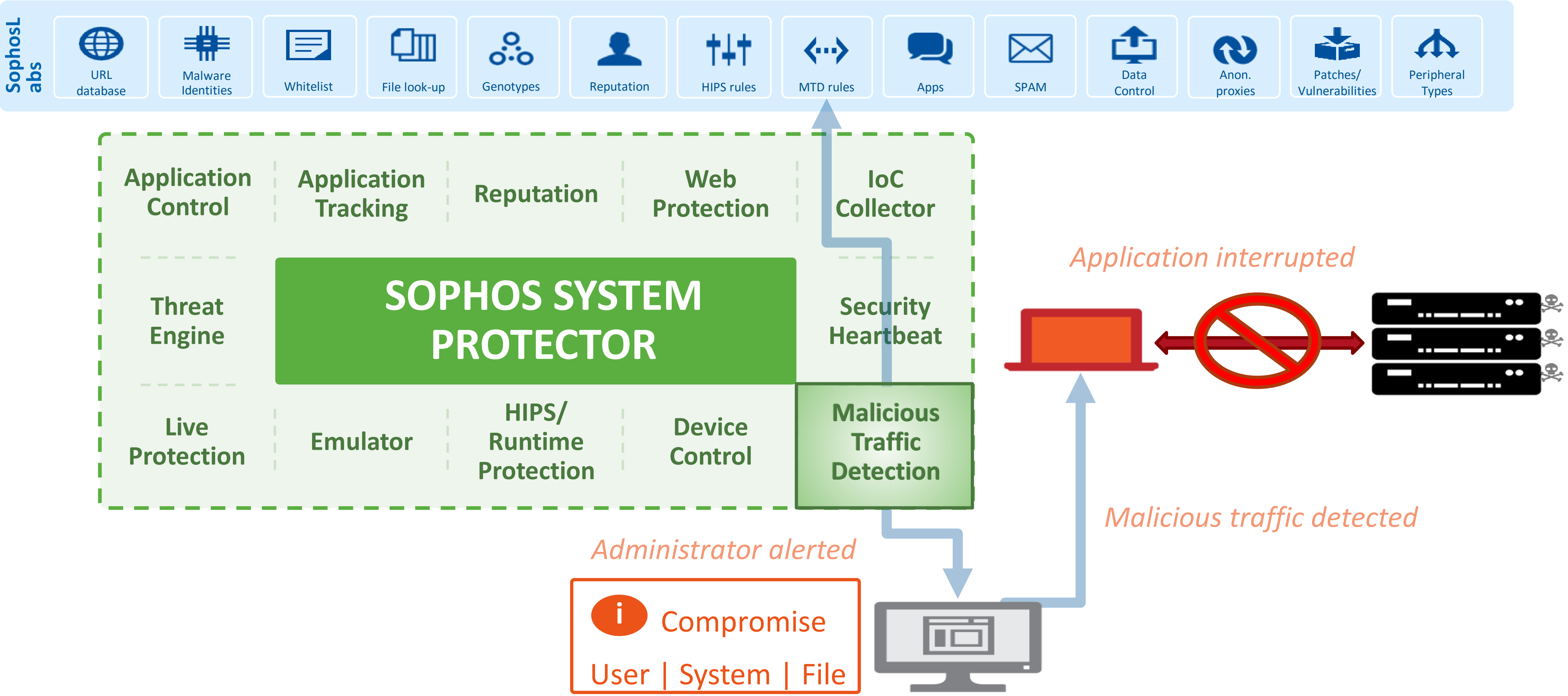
Security can be made simple
Platform, deployment, licensing, user experience

Synchronized Security

Integrated, context-aware security where Enduser and Network technology share meaningful information to deliver better protection



Malicious Traffic Detection



SophosLabs

URL database | Malware Identities | Whitelist | File look-up | Genotypes | Reputation | HIPS rules | MTD rules | Apps | SPAM | Data Control | Anon. proxies | Patches/ Vulnerabilities | Peripheral Types

SOPHOS SYSTEM PROTECTOR

Application Control | Application Tracking | Reputation | Web Protection | IoC Collector

Threat Engine | Security Heartbeat

Live Protection | Emulator | HIPS/ Runtime Protection | Device Control | Malicious Traffic Detection

Application interrupted

Malicious traffic detected

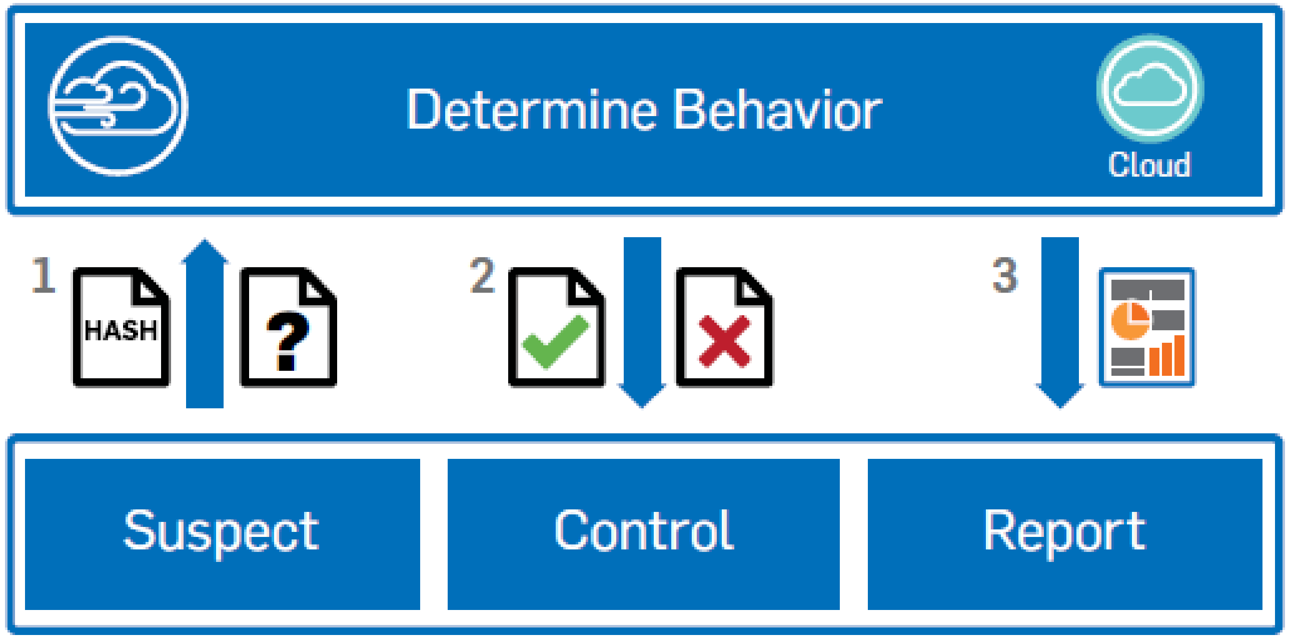
Administrator alerted

i Compromise

User | System | File

Sophos Sandstorm

Advanced Threat Defense Made Simple



Secure Web Gateway

Secure Email Gateway

Unified Threat Management

Next-Gen Firewall

How Sophos Sandstorm works

1. If the file has known malware it's blocked immediately. If it's otherwise suspicious, and hasn't been seen before, it will be sent to the sandbox for further analysis. When web browsing, users see a patience message while they wait.
2. The file is detonated in the safe confines of the sandbox and monitored for malicious behaviour. A decision to allow or block the file will be sent to the security solution once the analysis is complete.
3. A detailed report is provided for each file analyzed.

More information

- Sophos whitepaper on how to stay protected from ransomware
  https://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophosransomwareprotectionwpna.pdf?la=en
- Sophos technical whitepaper on ransomware
  https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf?la=en
- Naked Security – regular stories on Locky and other ransomware attacks
  https://nakedsecurity.sophos.com/
- IT Security DOs and DON'Ts
  https://www.sophos.com/en-us/medialibrary/PDFs/employeetraining/sophosdosanddontshandbook.pdf?la=en
- Threatsaurus
  https://www.sophos.com/en-us/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf?la=en
- Sophos free tools
  https://www.sophos.com/fr-fr/products/free-tools.aspx

SIGNATURE SYSTEMS, INC

PDQ

TECHNOLOGY SERVICES

SOPHOS