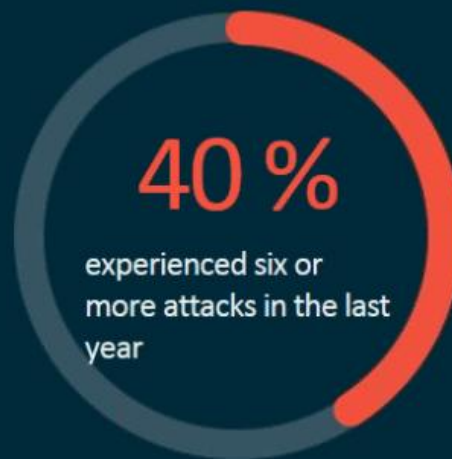


# Security and Business Continuity

Jamie Smith  
Lanetco Computer Networks Inc.

## Of 1,100 Solution Providers responding:



Less than 1 in 4 ransomware incidents are reported to the authorities



42% of report companies paid the ransom



1 in 4 who did so never recovered  
the data

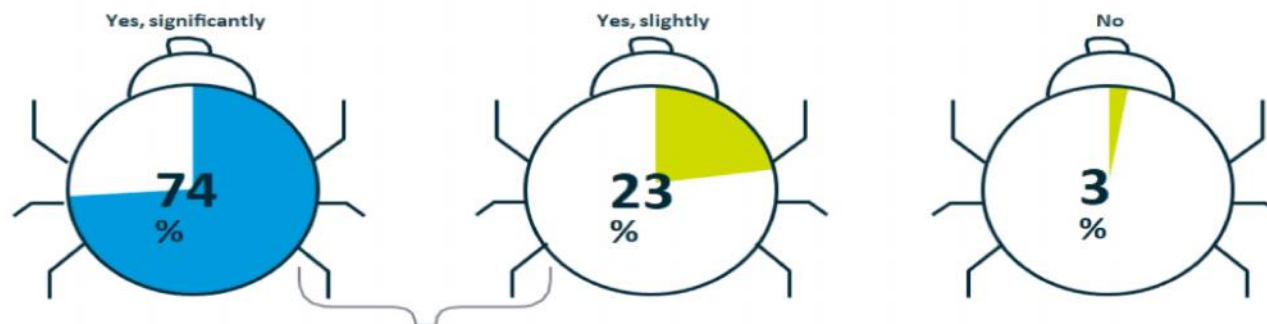


## MAJORITY OF IT SERVICE PROVIDERS AGREE: RANSOMWARE IS HERE TO STAY

► With which of the following statements, do you most agree?



► Will the # of ransomware attacks continue to increase over the next 2 years?



**97% predict these incidents will continue to increase.**



## THE SIGNIFICANT DISCONNECT BETWEEN THE IT SERVICE PROVIDER AND THE CLIENT ON RANSOMWARE

- How concerned are you about the threat of ransomware? How concerned are your small business customers?

Who is “highly concerned” about the threat?



**88%**  
of IT  
Pros

**Vs.**

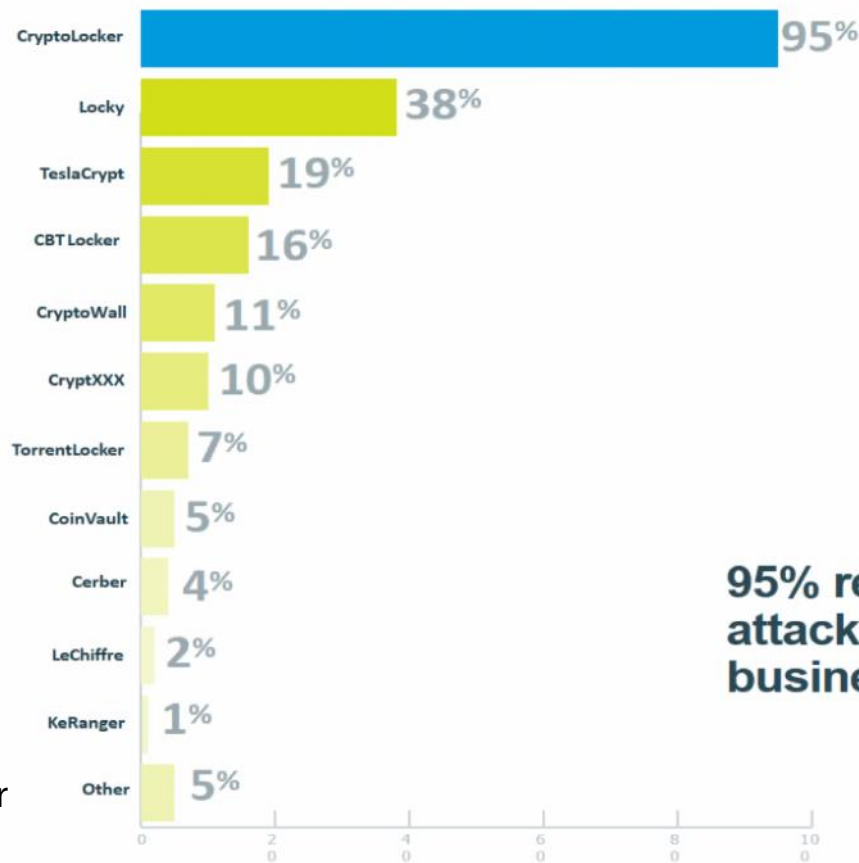


**34%**  
Of Small  
Business  
Owners

Datto Partner Survey 2016

## CRYPTOLOCKER IS KING

► Have any of your customers fallen victim to one or more of the following strains of ransomware? (Check all that apply)



**95% report CryptoLocker attacks against their small business customers.**



---

# SQL Application and Database Encryption

---

## Cerber Ransomware switches to a Random Extension and Ends Database Processes

By [Lawrence Abrams](#)

 October 4, 2016  6:20 PM  8

Late last week, a [new version](#) of Cerber Ransomware was released that included some new features. The most notable change is the switch from the static **.Cerber3** extension for encrypted files to a random 4 character extension, the use of a HTA file as the ransom note, and the termination of various database processes before encryption.

With this version, when a victim's files are encrypted, not only will the filename be scrambled, but the extension will be replaced as well. This means that a file that was previously encrypted as **5NgPiSr5zo.cerber3**, would now be encrypted to a name like **1xQHJgozZM.b71c**.

This version also includes a new ransom note called README.hta. When launched, the ransom note will appear in an application Window and display the normal ransom note. An example of the README.hta file can be found below.

---

# Security Breaches

## A New Headline Every Day

---

### U.S. to establish new cybersecurity agency

BY WARREN STROBEL

WASHINGTON | Tue Feb 10, 2015 10:12am EST

### Anthem Hacking Points to Security Vulnerability of Health Care Industry

By REED ABELSON and MATTHEW GOLDSTEIN

CEO heads may roll for security breaches in wake of Sony boss' exit, experts say

Feb 9, 2015, 6:54am PST

### Brokerage Firms Worry About Breaches by Hackers, Not Terrorists

By MATTHEW GOLDSTEIN FEBRUARY 3, 2015 11:54 AM 4 Comments

### Sony PlayStation and Microsoft Xbox Live Networks Attacked by Hackers

By NICOLE PERLROTH and BRIAN X. CHEN DECEMBER 26, 2014 4:11 PM 31 Comments

---

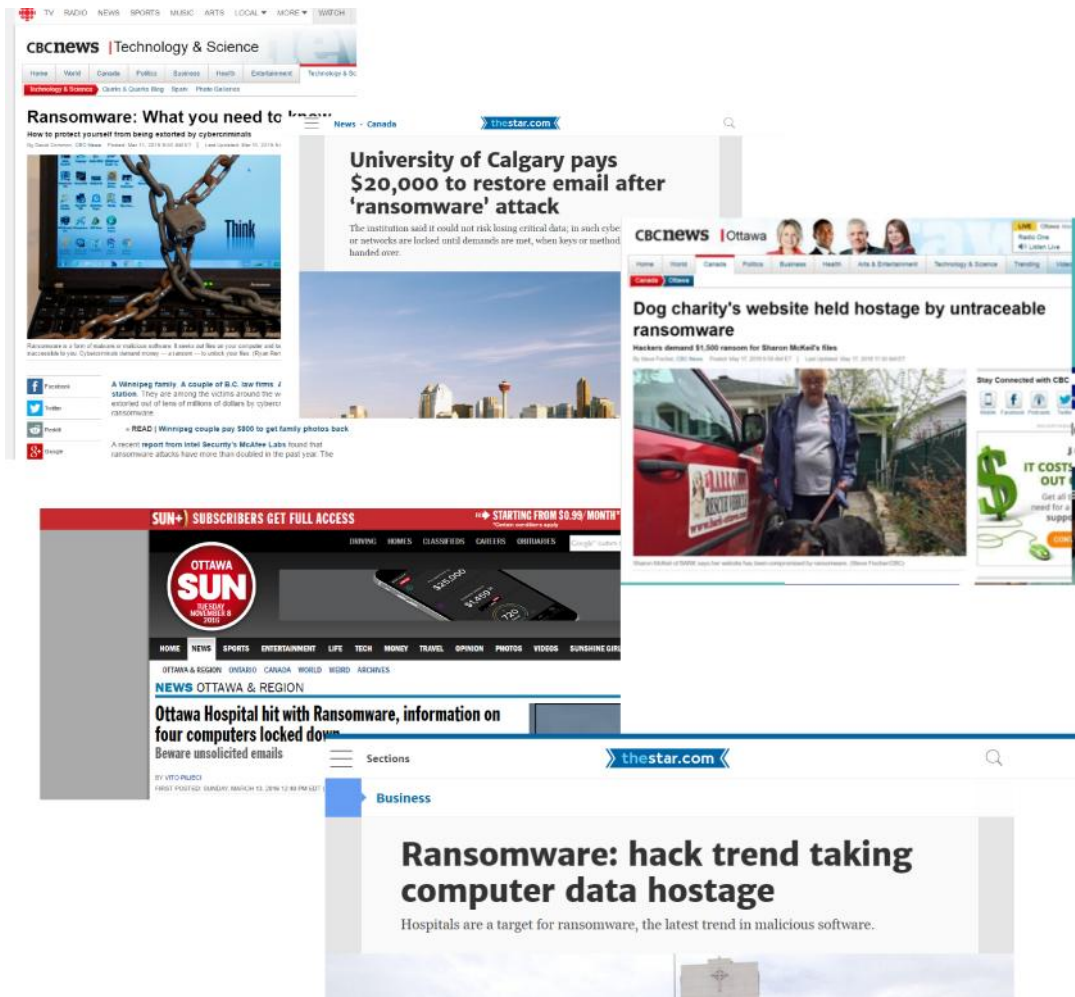
### *F.B.I. Says Little Doubt North Korea Hit Sony*

By MICHAEL S. SCHMIDT, NICOLE PERLROTH and MATTHEW GOLDSTEIN JAN 7, 2015

But Ransomware has taken over as the new real threat



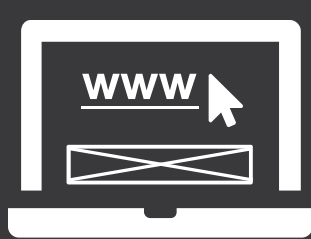
# Ransomware Security Breaches



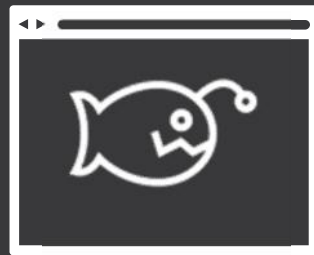


# Ransomware Under the hood

# Ransomware workflow



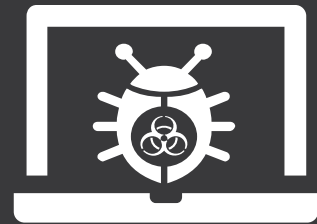
User Clicks an  
Email Link or  
Malvertising



Initial Exploit  
Typically Using  
Angler EK



Malicious  
Infrastructure



Ransomware  
Payload



# Emails are still popular and are getting better

**TACTIC**

Trick SMB into opening link or attachment

FedEx Service <details@fedex.com>  
To: [redacted]  
FedEx delivery problem # Error ID4900

August 13, 2012 6:54 AM  
[Details](#)



FedEx  
Federal

Unfortunately we  
package you have  
time because the  
erroneous.

Please print out the  
collect the package

[Print a](#)

<http://thetechguy.com/content/uploads/7.37.58-AM.png>

ADP

IN THE BUSINESS OF YOUR SUCCESS™

## ADP Prompt Information

Report ID: 85304

October, 22 2013  
Valued ADP Client

Company with ID 43962 Complete Payroll Transfer from your ADP account recently. I  
system:

[Access Activity Report](#)

Please overview the following notes:

- Please note that your bank account will be charged within one banking day for the sum sho
- Please Not try to reply to this message. automative notification syste  
Please Contact your ADP Benefits Authority.

This note was sent to current users in your system that access ADP Netsecure.



Thu 26/03/2015 10:49 AM

Santiago <Santiago [redacted] com>

Santiago Henson - My resume

To: [redacted]

Message

[Santiago Henson - My resume.zip \(4 KB\)](#)

Hi, my name is Santiago Henson  
I am herewith submitting my Resume under attachment for your perusal.

Thank you,  
Santiago

# How email is used in Ransomware


Link to  
Exploit Kit Drive  
by Download site

Dropper as  
Attachment

Ransomware  
Binary as  
attachment



# Malvertising Overtakes Porn for Web Infections



**“We found that at least 27 percent of the Alexa 1000 websites were delivering malware via malicious advertisements.”**

**Bromium Labs**

Endpoint Exploitation Trends 2015 H2

# Malvertising on the Rise

## How does malvertising work?

1. Set up a website with exploit kit
2. Run an ad on Yahoo, AOL or other ad network, with legitimate company creative
3. Ad server runs remote Flash exploits or redirects users to exploit kit site
4. User gets infected

Attn: NYTimes.com readers:  
Do not click pop-up box  
warning about a virus – it's  
an unauthorized ad we are  
working to eliminate.

**The New York Times**

Top websites deliver  
CryptoWall ransomware  
via malvertising...

**Adam Greenberg**  
SC Times



# Malvertising Using Hijacked Images to Target SMBs

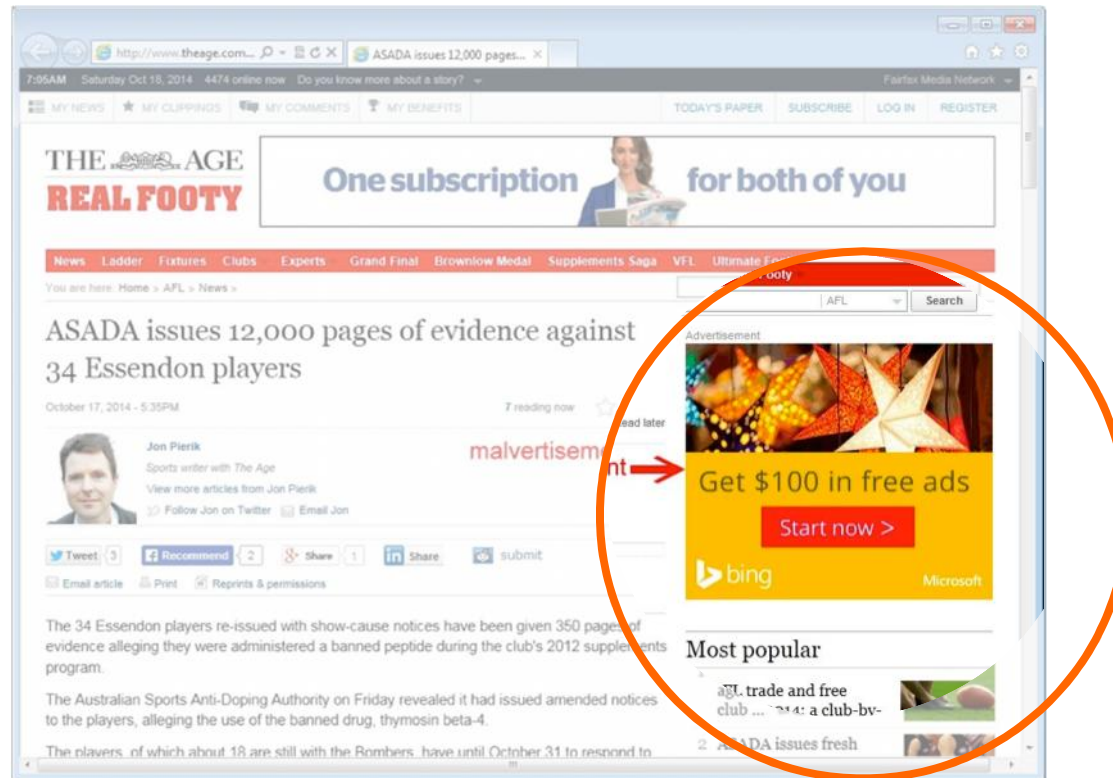


Image: [http://news.softpedia.com/news/CryptoWall-2-0-Delivered-Through-Malvertising-On-Yahoo-and-Other-Large-Sites-462970.shtml#sgal\\_0](http://news.softpedia.com/news/CryptoWall-2-0-Delivered-Through-Malvertising-On-Yahoo-and-Other-Large-Sites-462970.shtml#sgal_0)



## Recent examples of malvertisers hijacking legitimate ads

Prosper Loans malvertising:  
CBS TV websites in  
St. Louis, MO and Charlotte, NC

**NEED A SMALL  
BUSINESS LOAN?**

LET YOUR PEERS INVEST IN YOUR BUSINESS  
THROUGH PROSPER TODAY

RATES AS LOW AS:  
**6.73%**  
APR\* **PROSPER**

<https://blog.malwarebytes.org/?p=12525>

Roadkill T-shirts malvertising:  
Rotten Tomatoes, Autoblog  
Jerusalem Post and more



<http://blog.malwarebytes.org/?p=10983>

Hugo Boss malvertising:  
Huffington Post



<https://blog.malwarebytes.org/?p=7547>

LiveDrive (backup) fake ad: NY Daily Post

Start your **FREE**  
14 day trial today

Sign up now

**livedrive**

<https://blog.malwarebytes.org/?p=7368>

Image Creator malvertising: Match.com



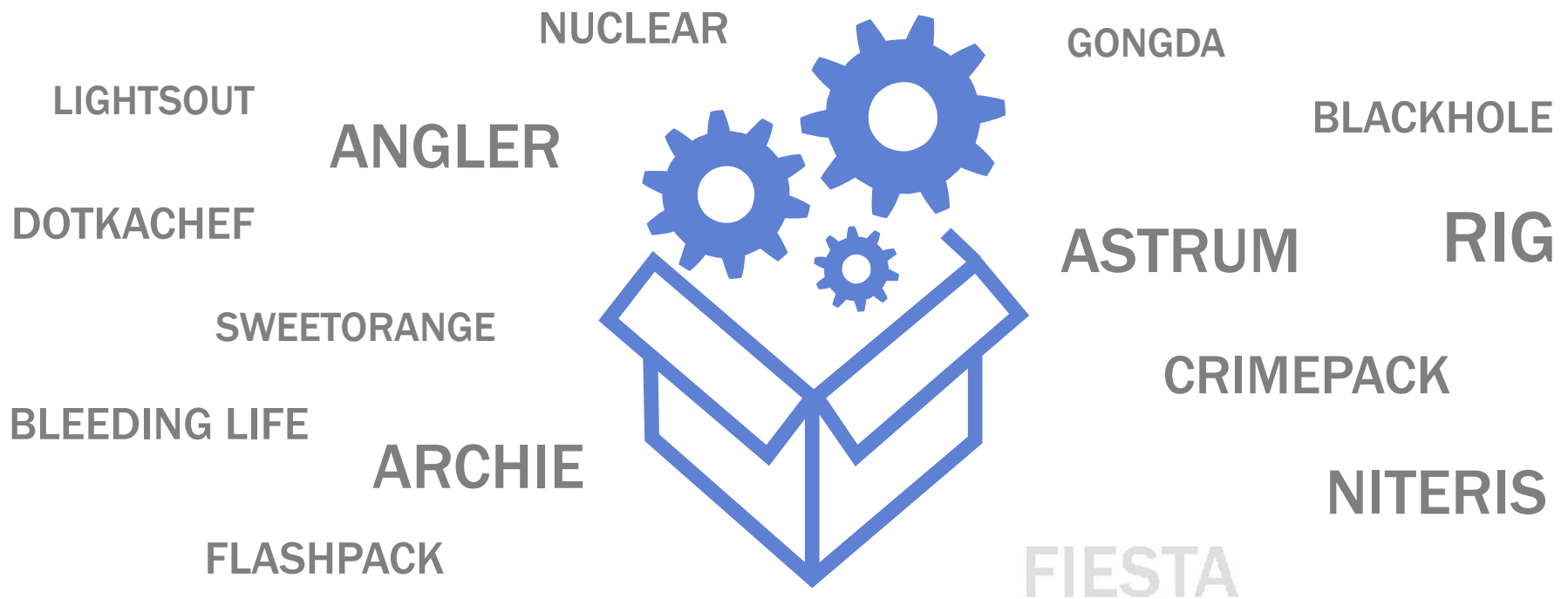
<https://blog.malwarebytes.org/?p=9389>

A photograph of three people in an office environment. A woman with dark hair in a bun stands behind a man and a woman seated at a desk. The man is looking at a laptop screen, and the woman is gesturing with her hands while speaking. The scene is dimly lit with a soft glow from the laptop and background lights.

What's an exploit kit?

## Explosion in SaaS/CaaS Plug-and-Play Marketplace

Kits cost as little as \$200



# Exploit Kits Are Getting Better



<http://krebsonsecurity.com/2010/10/java-a-gift-to-exploit-pack-makers/>

## 14 'Blackhole' Exploit Kit Author Gets 7 Years

APR 16

A Moscow court this week convicted and sentenced seven hackers for breaking into countless online bank accounts, including "Paunch," the nickname used by the author of a widely used exploit kit. Once an extremely popular crimeware-as-a-service, the kit was responsible for a large percentage of malware infections, and likely contributed to tens of millions of dollars in losses over several years.

"According to Russian security firm Group-IB, Paunch had more than **1,000 customers** and was **earning \$50,000 per month** from his illegal activity."

news  
The 27-year-old was arrested along with an entire team of other cybercriminals who worked to sell, develop and profit from Blackhole.

According to Russian security firm **Group-IB**, Paunch had more than 1,000 customers and was earning \$50,000 per month from





# Cisco Umbrella DNS

Diverse Set of Data &  
Global Internet Visibility

**80B**

Requests  
Per Day

**160+**

Countries

**65M**

Daily Active  
Users

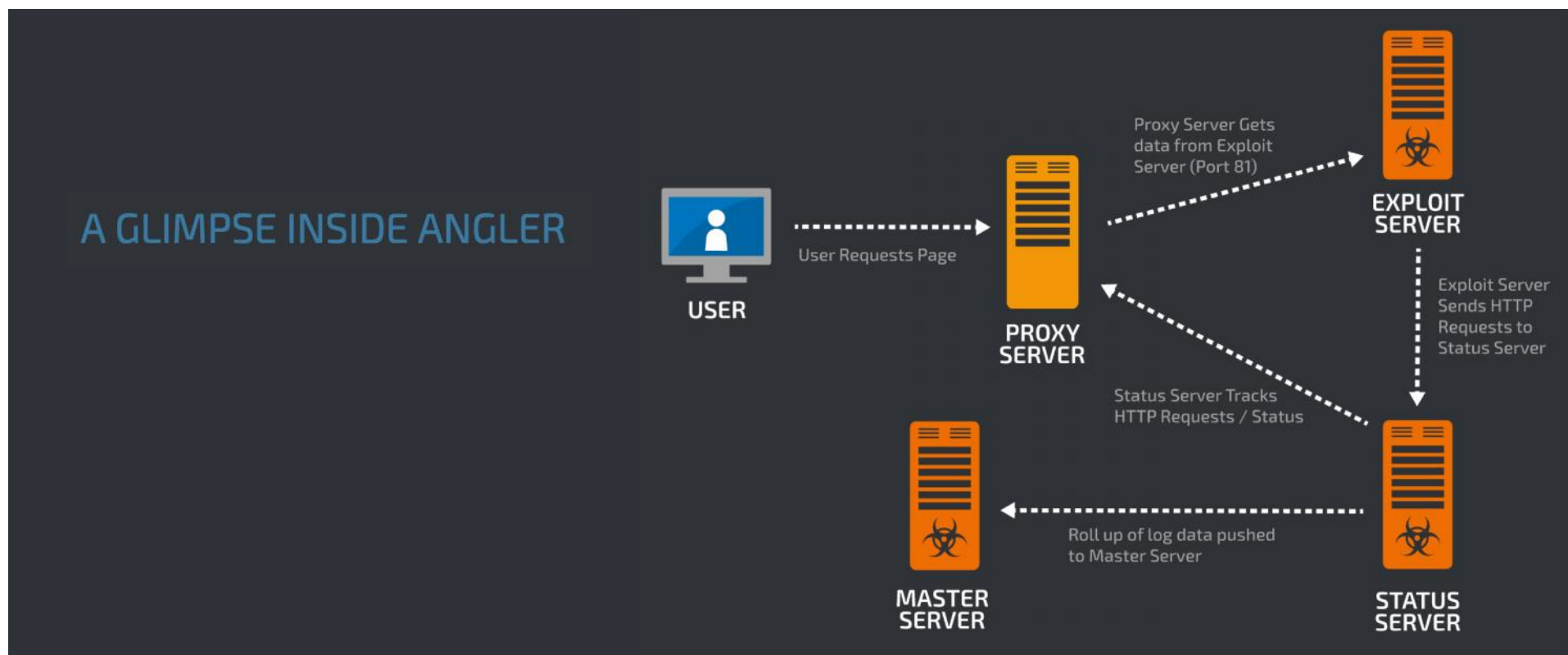
**10K**

Enterprise  
Customers





## Angler Exploit Kit has taken over — especially for ransomware



## Angler has truly exploded in volume



90,000

targeted victims per day



9,000

observed served exploits  
in a single day



40%

of users being served  
exploits were  
compromised



62%

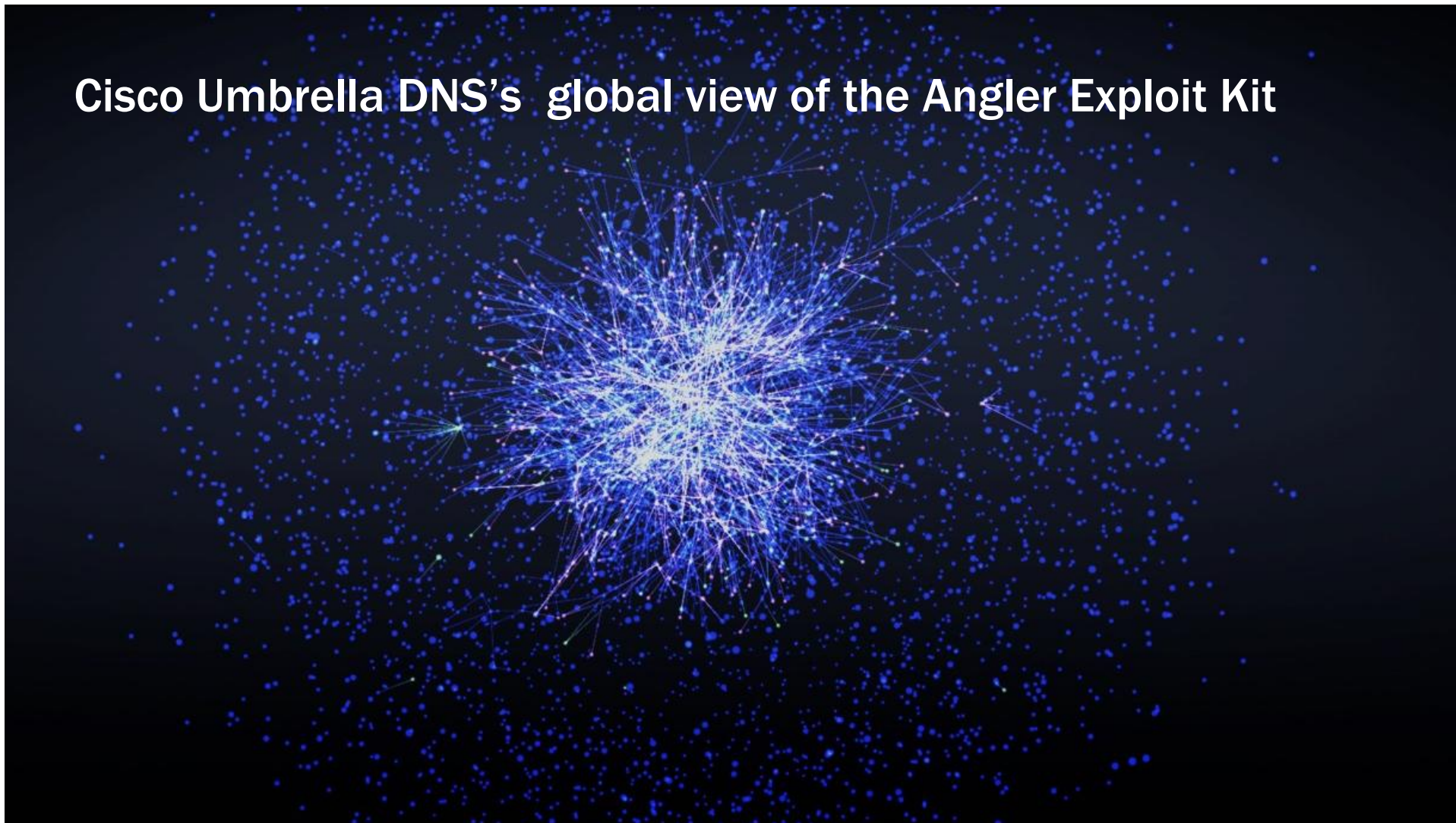
of Angler infections  
delivered Ransomware

“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** activity associated with the adversaries.”

### **Angler Exposed**

Cisco Talos and OpenDNS labs

## Cisco Umbrella DNS's global view of the Angler Exploit Kit





using modern data analysis to surface threat activity in unique ways

using modern data analysis to surface threat activity in unique ways



A man in a dark suit is walking from left to right, pushing a red hand truck. The hand truck is loaded with several cardboard boxes, some of which are secured with blue straps. The background is a blurred city street with cars and buildings, suggesting motion. The text "Intermediate step: Dropper Malware" is overlaid in white, bold, sans-serif font on the left side of the image.

# Intermediate step: Dropper Malware



## Increasingly Common Step: Dropper

Increasingly Common Option for Ransomware

### > TACTIC

Malware that  
installs other  
malware

1

Bad actor gets a  
piece of malware  
on computer

2

Malware sits  
quietly and just  
phones home; not  
the flashy/noisy  
malware

3

Bad actor sells or  
rents ability to  
infect computer

- Malware phones home
- **Installs main payload: Ransomware, Keylogger, Spambot**

4

If contract  
ends or more  
capacity,  
install more  
malware

[Show filter options](#)

0 1 2 &gt; &gt;&gt;

Bot ID	Bot name	IP address	OS	Serial key	Antivirus	Country	Version	Quality	Status	Action
9d93cc2243542e6af53bcd4ae029240	380DDB1701933E80		Windows 7 Ultimate (x64)				2.4		online	
15248c10b9928704048fc999129ff5fd	51E0VOCKAZ1N6C1		Windows 8 (x64)				2.4		online	
c8e908e7632d1821c3460590766f7475	CQEDH9893KFO31K		Windows 7 (x32)				2.4		online	
e1ef97fd054cdfd32cc05d937b6cb53c	EX0LSC26LRWO82U		(NAT) Windows XP (x32)				2.4		online	
24b2c8e794a28e01e7b6c614dd764e88	X2NQ4VBZK790AXW		Windows 7 (x32)				2.4		online	
f4c53baeebd0dcd16e4774e952963949	VKIP16A6MSBEP0G		Windows XP (x32)				2.4		online	
71d3402db1db2ce6e33b6e9ca9fc65e2	9ARE00T1EDQFGUC		(NAT) Windows Srv 2008 (x64)				2.4		online	
e040e92f8e9b191798813b8ea5462dc8	SMJ9Q5EFELCN5NK		Windows 8 (x64)				2.4		online	
c0f565b6be5fe40fa24689ab9b18403f	728F0W03KVVW5X2		Windows 7 (x64)				2.4		online	
f9a0b22343e060b771c8027ba7f51c95	2JZIO0P5W79B7ZQ		Windows 7 (x32)				2.4		online	
9ff4d1b86e009ad4a960edb2f8d933d4	ZACZCDFG9TL8WDE		(NAT) Windows Srv 2008 (x64)				2.4		online	
68633b16c634e5679a3e3a9df746dac9	D1ESH6SR8L51XO1		Windows Srv 2008 (x64)				2.4		online	
694dafd2f6ff0a1d817eca6566b54ef9	AE8S73PCYZP4R7W		Windows XP (x64)				2.4		online	
a9f0f17550b781d47321d0914e9df641	PKXC0LYMX9NR8N7		(NAT) Windows 7 (x64)				2.4		online	
9aae59e68a40469a62704c168f646686	ZZDQ195L5HNV73J		(NAT) Windows 8 (x64)				2.4		online	
2ed6f1763afd2e605ae532f0139711ec	YRWLINUI58QZ2U2		(NAT) Windows 7 (x32)				2.4		online	
23d2427831edd700f956d9cddb31d4c3	2OQI95AHMKRHZHW		(NAT) Windows Srv 2008 (x64)				2.4		online	
f1407afde98c0c1a404e5771a1ab9ad9	H5HBELQVKZKYRFR		Windows 7 (x32)				2.4		online	
6b34c4125577f30f9681b747227b00ef	IGDBIBPJLURXNDS		6 (NAT) Windows Srv 2008 (x64)				2.4		online	
9ed05e0b0c1e8b9dac920bab8261c1d2	8DHPUI9JXI2XOC0		Windows XP (x64)				2.4		online	
97421540e8d06b671bc4fe18112767e	1H7LY7URDQ1Q607		(NAT) Windows 7 (x64)				2.4		online	



Приветствую всех!

**Greetings to all!**

В связи с неожиданным переизбытком, продам не нужные инсталлы.

**Due to overstock I am selling unneeded installs.**

Цена : 60 вмз за 1к

**Price: \$60 WMZ for 1k**

Оплата: оплата вперед, без протекции.

**Payment: In advance, with no escrow.**

География: микс мира, практически без азии.

**Geography: A mix of countries, with virtually no Asia.**

Что грузится: грузится на бота только мой граббер и ВАШ спамбот (ничего кроме спамботов не грузю принципиально)

**Loads: Only my grabber and your spam bot is being loaded (nothing but spam bots allowed)**

Получение: оплачиваете и через 10 минут я запускаю Ваш exe на прогруз.

**Delivery: You pay and I start running your exe in 10 minutes.**

Качество: исходя из того, что я написал выше, я не грузю ничего кроме своего граббера и вашего спамбота, загрузки не дохнут и я никого не выгружаю со временем, не грузю по 2 exe на 1 бота. Хотя о качестве я думаю отпишут те, кто брал у меня уже инсталлы.

**Quality: As stated above, nothing else is loaded besides my grabber and your spambot, loads do**

Контакты: **not die, and I do not overutilize resources, or load 2 exe per bot. Inquire with others who have already purchased installs**

icq: 312-456, когда стучитесь, просьба сообщать ваш ник и что вы с форума по поводу инсталлов.

Всем спасибо, приятного дня.

качество: исходя из того, что я написал выше, я не грузю ничего кроме своего граббера и вашего спамбота, загрузки не дохнут и я никого не выгружаю со временем, не грузю по 2 exe на 1 бота. Хотя о качестве я думаю отпишут те, кто брал у меня уже инсталлы.

**Quality: As stated above, nothing else is loaded besides my grabber and your spambot, loads do**

Контакты: **not die, and I do not overutilize resources, or load 2 exe per bot. Inquire with others who have already purchased installs**

icq: 312-456, когда стучитесь, просьба сообщать ваш ник и что вы с форума по поводу инсталлов.

Всем спасибо, приятного дня.

Source: krebsonsecurity.com

## Price Per Infection/Infection as a service

Region	2015 Average Price per 1,000 Infections	2015 Average Price per install
US	\$70	\$0.07
Europe	\$105	\$0.11
Asia	\$140	\$0.14
Australia	\$140	\$0.14

Data from Trend Micro Report: “Russian Underground 2.0”



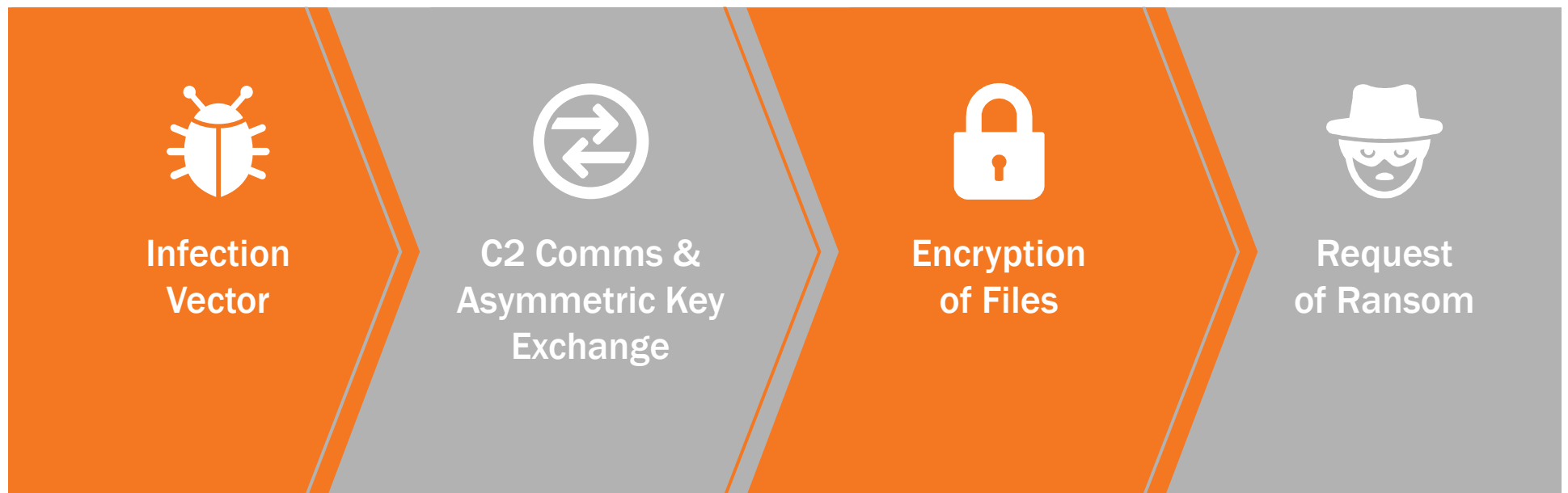


Ransomware  
payload
















# Typical Ransomware Infection

At a high level



Encryption C&C

Payment MSG

NAME	DNS	IP	NO C&C	TOR	PAYMENT
Locky					DNS
SamSam					DNS (TOR)
TeslaCrypt					DNS
CryptoWall					DNS
TorrentLocker					DNS
PadCrypt					DNS (TOR)
CTB-Locker					DNS
FAKBEN					DNS (TOR)
PayCrypt					DNS
KeyRanger					DNS

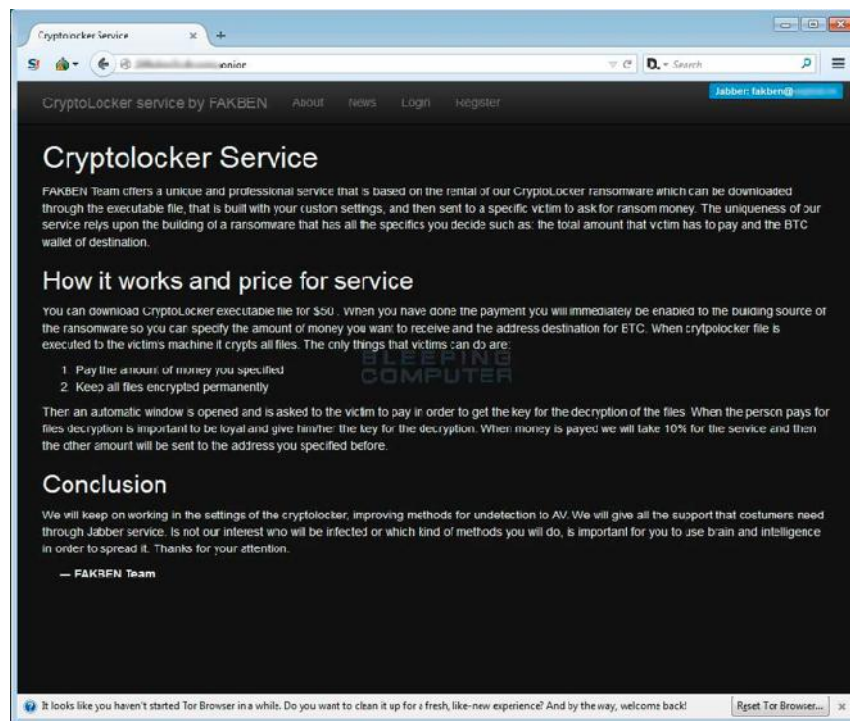
# Your files are encrypted!

## And you are asked for a ransom to get them back

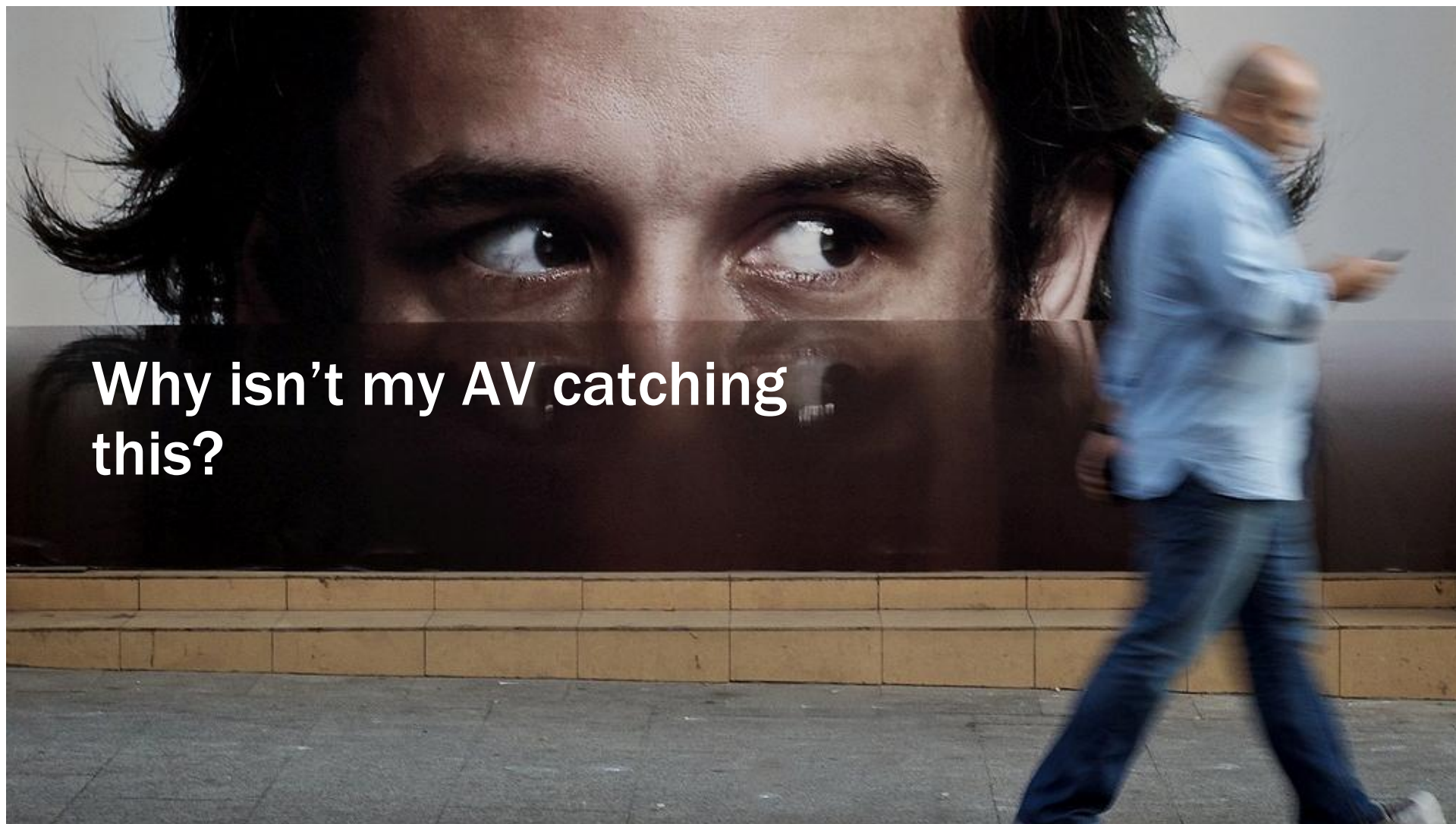


# Now available as a reseller model!

Non techie cybercriminals can partner and keep 80% of revenue







**Why isn't my AV catching this?**



**“Signature-based tools (antivirus, firewalls, and intrusion prevention) are only effective against 30–50% of current security threats.”**

**IDC**

November 2011

## Getting Around Signatures: Crypters



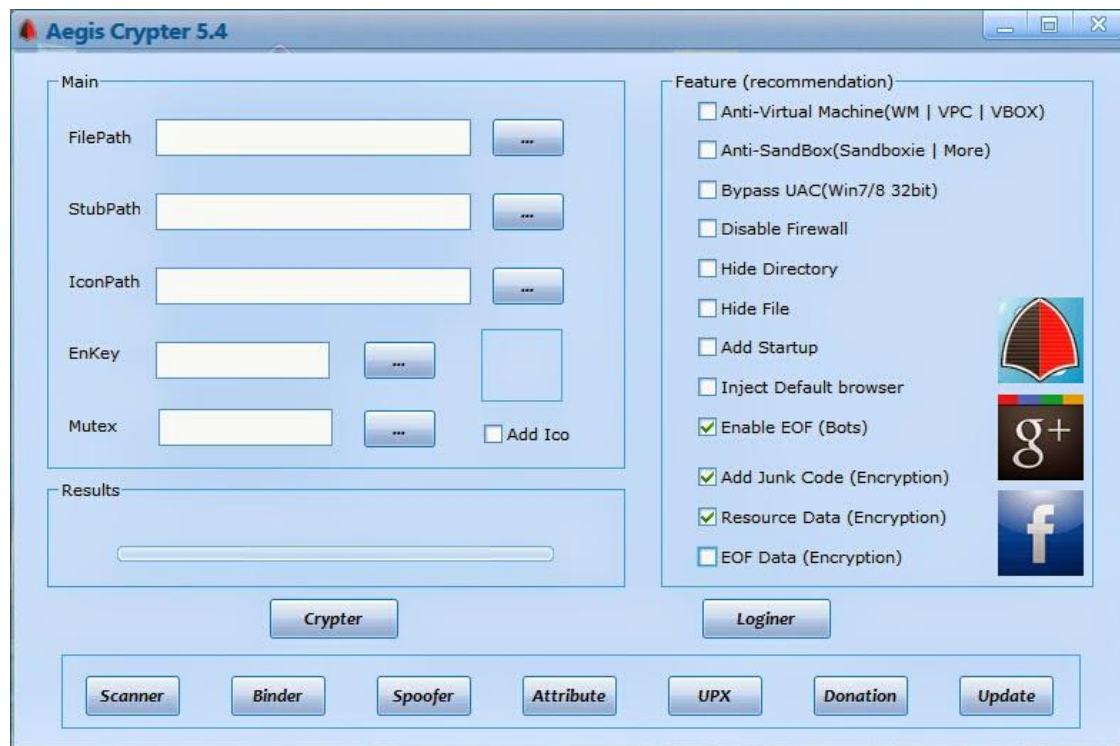
Bypass 35 AV's in Under 3 Minutes

## Getting Around Signatures: Crypters

### **Protect your files and remove false detections!**

We provide encryption software to protect files against invaders and remove false positive detections. We are leading the market with multiple FUD Crypters and cryptography solutions.

# Getting Around Signatures



<http://buy.aegiscrypter.com/>

# Test Against Signature Based Tools

Type link or choose file

Choose

Scan

Done

File name: 34.exe (156 KB)

Result: 2/39

Started at: 15-04-15 08:12:17 UTC

Duration: 9 seconds

show by files

Antivirus	Results
Ad-Aware Pro	Clean
AhnLab V3 Internet Security	Clean
ArcaVir Antivirus 2014	Clean
avast! Internet Security	Clean
AVG Anti-Virus	Clean
Avira Antivirus Suite	Clean
BkDefender Antivirus Plus 2015	Clean
BullGuard Antivirus	Clean
Clim AntiVirus	Clean
COMODO Antivirus	Clean
Dr.Web Anti-virus	Clean
Emsisoft Anti-Malware	Clean
eScan Antivirus	Clean
ESET NOD32 Antivirus	Clean
F-PROT Antivirus for Windows	Clean
F-Secure Internet Security 2014	Clean
FortiClient Lite	Clean
G Data AntiVirus	MSIL.Trojan.Stormik.B (Engine B)
IKARUS anti-virus	Clean
Jiangmin Antivirus 2011	Clean
KT UltimateSecurity	Clean
Kaspersky Anti-Virus 2015	Clean
Malwarebytes Anti-Malware	Clean
McAfee VirusScan Enterprise	Clean
Microsoft Security Essentials	Clean
Nano Antivirus	Clean
Norman Security Suite	Clean
Outpost Antivirus Pro	Clean
Panda Global Protection 2014	Clean
Quick Heal Internet Security	Clean
Sophos Anti-Virus	Mal/MSIL-KG
Symantec Endpoint Protection	Clean
Total Defence Anti-Virus 2011	Clean
Trend Micro Titanium iS	Clean
TrustPort Antivirus	Clean
Twister Antivirus	Clean
VBA32 Anti-Virus	Clean
VIPRE Internet Security 2015	Clean
Zillya Internet Security	Clean

<http://www.aegiscrypter.com/>

## Why is CypherX The Best Crypter to Buy?

nent and testing for over 3 years. During this period we have pushed the limits with undetectable softwa  
s an advantage that allows us to more effectively keep files fully undetected from analysis, reverse engin

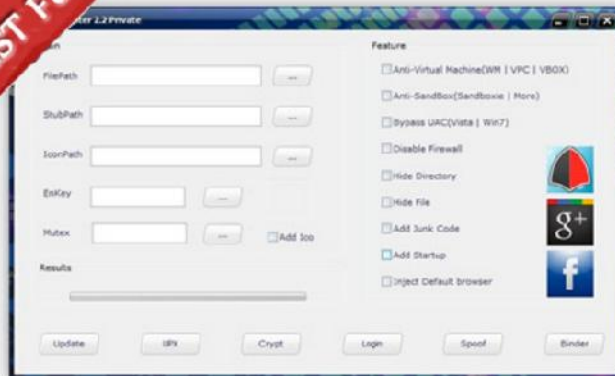
Download CypherX now and make files undetectable from:





## Aegis Crypter Purchase plan

**BEST FUD**



### Aegis Crypter Main Feature

- ✓ **Anti-Virtual Machine**
- ✓ **Anti-SandBox**
- ✓ **Add Startup**
- ✓ **Inject browser**
- ✓ **Bypass UAC**
- ✓ **Stub Update**
- ✓ **UPX Compression**
- ✓ **Spoof Extensions**
- ✓ **Files Binder**
- ✓ **More.....**

**Purchase**



#### Public version

**\$ 0** /month

**Free forever**

Good

#### Private version

**\$ 30** /month

**Need payment**

Better

#### Unique stub

**\$ 100** / unique stub

**Need payment**

Best

Public version	Private version	Unique stub
<p><b>\$ 0</b> /month</p> <p><b>Free forever</b></p> <p>Good</p> <p>No guarantee</p> <p>Anti-virus detection [FUD]</p> <p>—</p> <p>Technical Support</p> <p>—</p> <p>handsel</p>	<p><b>\$ 30</b> /month</p> <p><b>Need payment</b></p> <p>Better</p> <p>Keep &gt; 90%</p> <p>Anti-virus detection [FUD]</p> <p>—</p> <p>Technical Support</p> <p>FUD Java drive by</p> <p>handsel <b>payment&gt;\$100</b></p>	<p><b>\$ 100</b> / unique stub</p> <p><b>Need payment</b></p> <p>Best</p> <p>Must = 100%</p> <p>Anti-virus detection [FUD]</p> <p>✓</p> <p>Technical Support</p> <p>FUD Java drive by</p> <p>handsel</p>



**Won't the government  
protect me?**



# Government Guidance: Put better locks on your door


## Leadership and IT Professionals

- Implement Defence-in-Depth: layered defence strategy includes technical, organizational, and operational controls.
- Establish clear policies and procedures for employee use of your organization's information technologies.
- Implement Technical Defences: firewalls, intrusion detection systems, and internet content filtering.
- Update your anti-virus software daily.
- Regularly download and install vendor security "patches" for all of your software.
- Change the manufacturer's default passwords on all your software.
- Monitor, log, analyze, and report successful and attempted intrusions to your systems and networks.

If you have not paid ransom, call the Canadian Anti-Fraud Centre 1-888-495-8501

If you have paid ransom, you can report to your local police force





**“The ransomware is that good... To be honest, we often advise people just to pay the ransom.”**

**Joseph Bonavolonta**

Special Agent, FBI Cyber Intelligence






**“Paying the ransom does  
not guarantee the release  
of files.”**

**CCIRC**


CCIRC AL16-005



**“...results in unauthorized disclosure of personal information...statutory breach reporting obligation...”**

**Alberta Privacy Commission**

March 2016 – Alberta Personal Information Protection Act



**“Breach reporting  
obligations...added to  
CFPIPEDA, but those  
provisions are not yet in  
force.”**

**Borden Ladner Gervais**

The background of the slide is a dark teal color with a bokeh effect of out-of-focus light circles in shades of yellow, green, and blue. A faint, stylized DNA double helix is visible on the left side, extending diagonally across the frame.

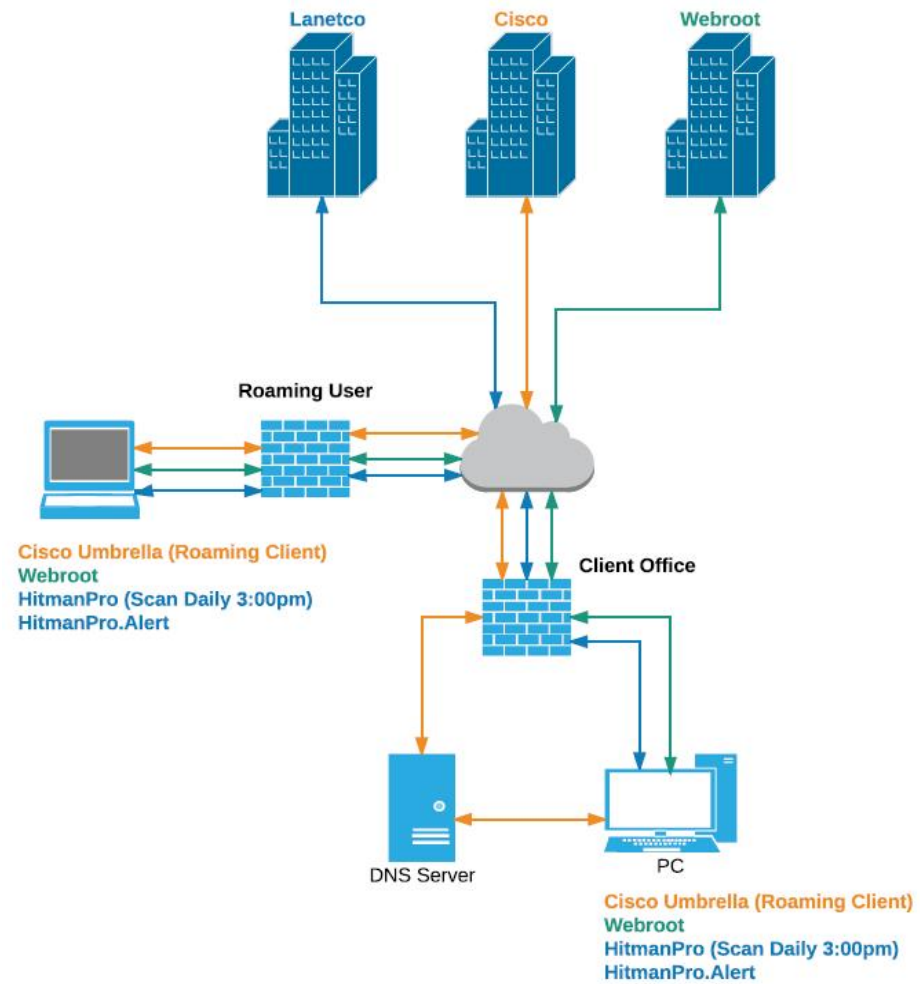
# Reducing risk of Ransomware

# PREVENT: Malware

- Protect users across the full infection chain
  - NOT JUST AN EXECUTABLE OR SIGNATURE
- Block sites with exploit kits at the network layer
  - Whether it's a whole site or an embedded ad
- Protect users from phishing attacks
  - To prevent breaches
- Block malicious links in emails and applications
  - Because the browser is not the only path of infection



# PREVENT: Malware

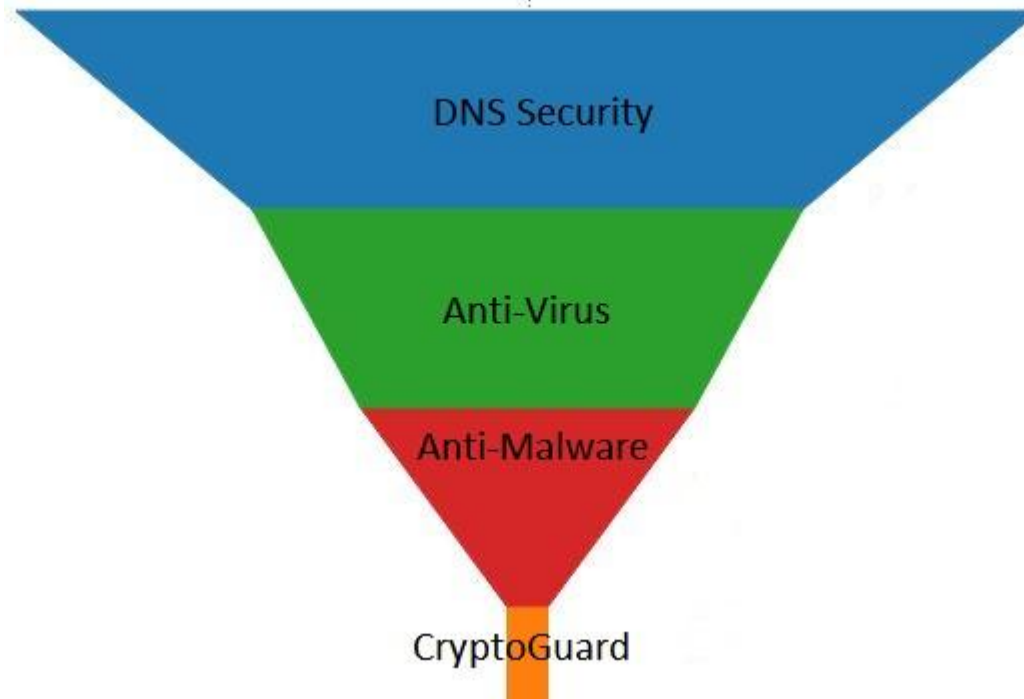


# CONTAIN: the new prevention

Prevent “Phoning home”

- Block “droppers” from getting malware
  - Whether it’s ransomware, keyloggers, spam senders or DDoS bots
- Stop Spyware/Keyloggers from uploading data
- Prevent Ransomware from getting an Encryption Key
- **Alert – and have team respond to alert**

## Contain: the new prevention



# TRAINING: educate

What we're doing today is important

- Help employees understand the threat — and the need to be vigilant
- Explain the cybercrime business — you aren't too small to be targeted
- If you see something strange, raise your hand!
- Tell others!

## TRAINING: educate

- Employee security training. Provides online, engaging, security awareness training and testing, confirming that your staff have completed the curriculum.
- Enhanced breach prevention. Testing by sending simulated phishing scams and ransomware to your employees. Weekly micro-training videos. Monthly security letters to employees. Written and easy to understand employee policies and procedures.



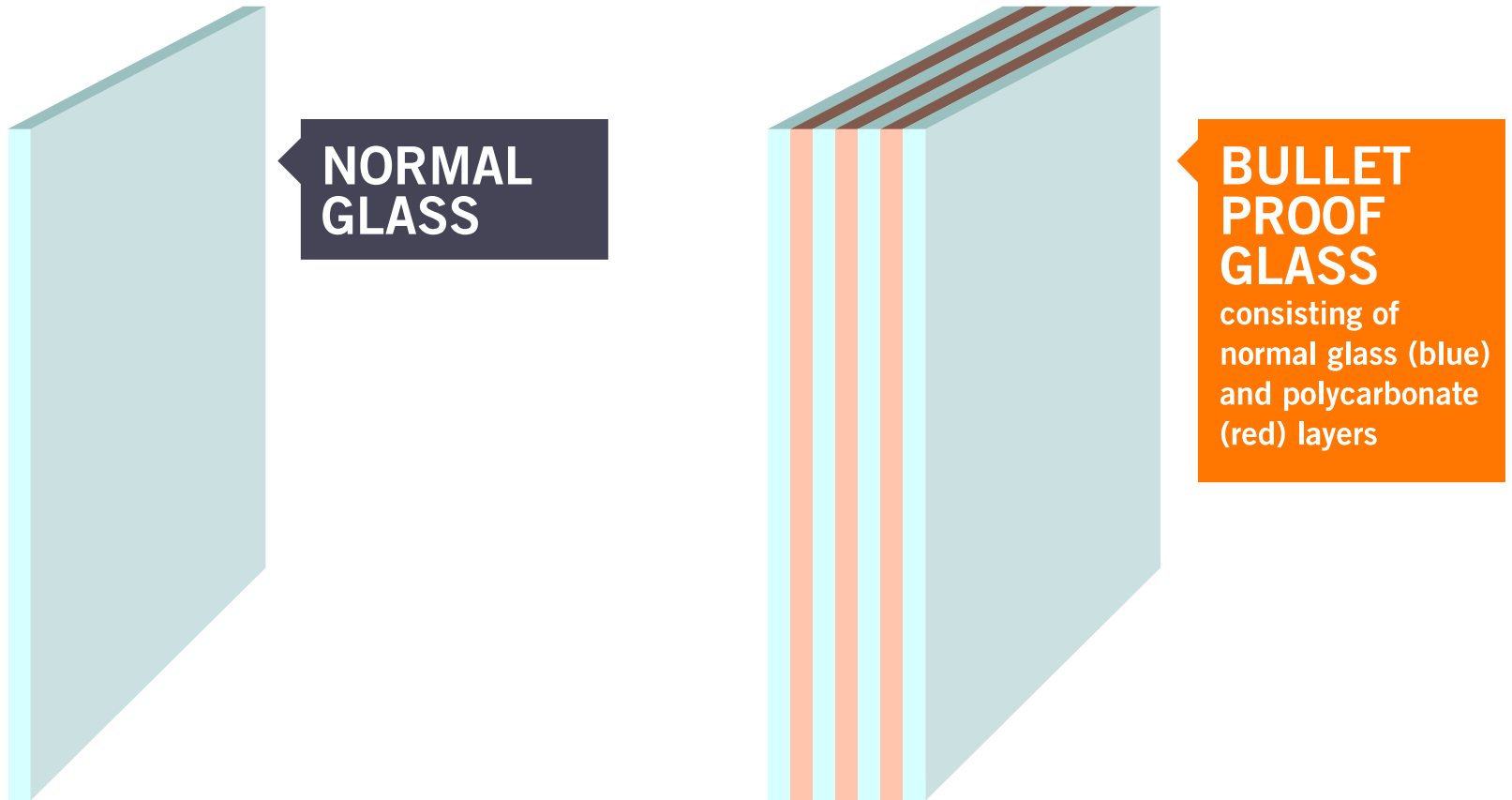
## **Backup:** the final layer

- Backup of data
- Multiple backup copy retention
- Offsite copies
- End user mobile File Sync and Share

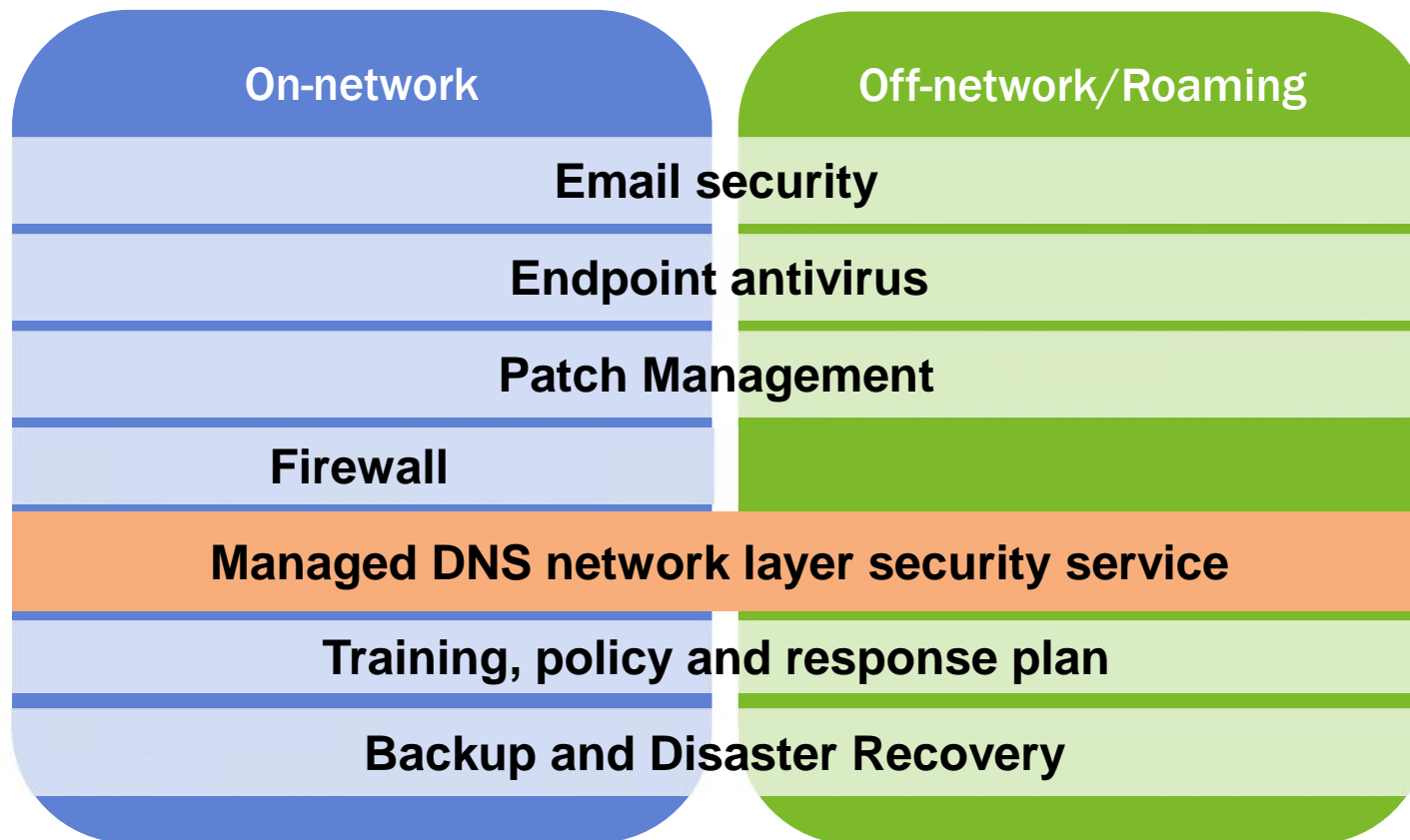
# Backup: the final layer

- Lanetco uses Backup and Disaster Recovery devices.
- Image based backup
- Local and offsite copy
- 12 month retention (5 daily, 4 weekly, 12 monthly)
- Built in Ransomware detection
  - Not an anti-virus or anti-malware tool
  - If files did exist and now drop to 0 (deletion)
  - Evaluate entropy of randomly selected files (if you had 1000 files with extension .PDF and now have 0)
  - Evaluate modification time vs create time on MBR
- End user File Sync and Share

## Security & risk mitigation: a layered approach



## Security is about managing risk through layers



## General Best-Practices

- Solid patch management
- Users run as non-privileged users (no admin)
- Disable RDP
- Firewall enabled on endpoints
- Segmented and secured backups (tested)



## For your home use:

- Install Windows, Java, Flash and Adobe Updates FREE!
- Install an anti-malware tool such as Malwarebytes.com (freemium) FREE!
- Install a DNS management tool such as OpenDNS.com (freemium) FREE!
- Sign up for, install and save your documents to a File Sync and Share (OneDrive, GoogleDrive, Syncplycity, DattoDrive, etc.) FREE!
- Use PassKey to store and create your passwords (different password per website) FREE!
- Upgrade the version of your anti-virus, and use a PAID FOR A/V
- Update your anti-virus daily

The background of the slide is a warm, golden-brown color with a bokeh effect. It features numerous out-of-focus circular light spots in shades of yellow, orange, and light brown, creating a soft, glowing texture. The text "Thank You!" is centered on the left side of the image.

**Thank You!**



Questions?