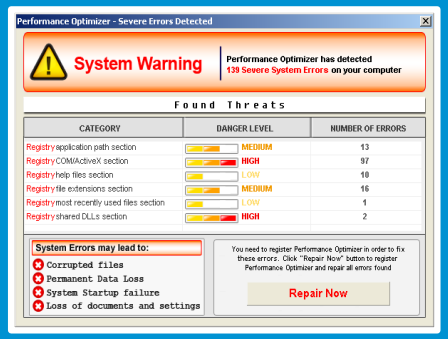
# Ransomware

**Bill Wright**
**Symantec Government Affairs**

# Evolution path

## MISLEADING APP




## FAKE AV


## LOCKER RANSOMWARE

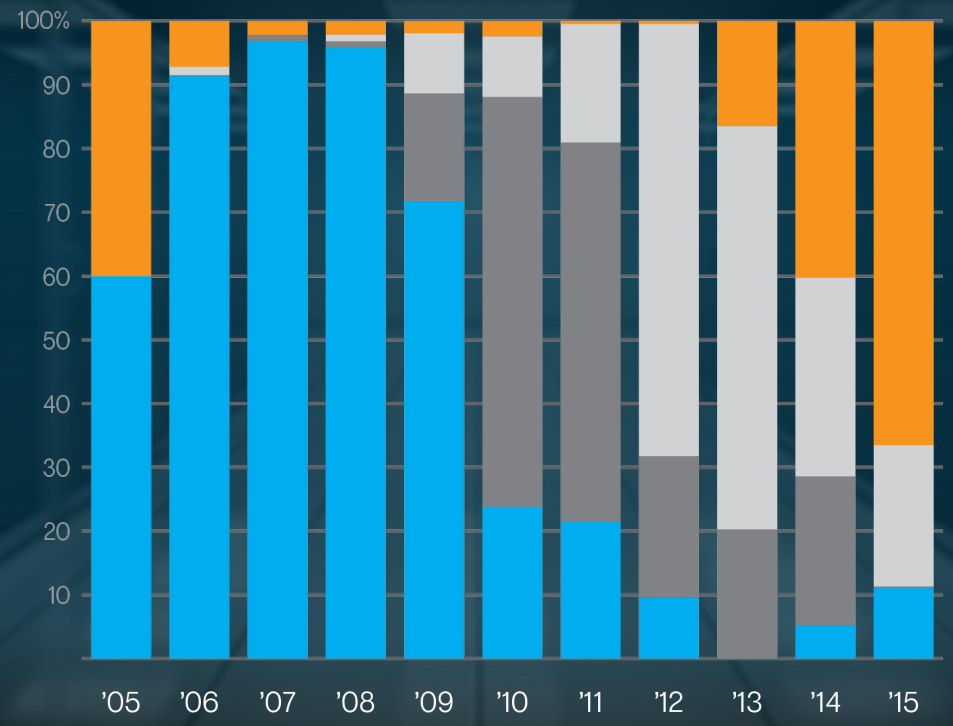

## CRYPTO RANSOMWARE


**2005-2009** → **2010-2011** → **2012-2013** → **2014-2015**

**"FIX"** | **"CLEAN"** | **"FINE"** | **"FEE"**

# Growing Dominance of Crypto-Ransomware

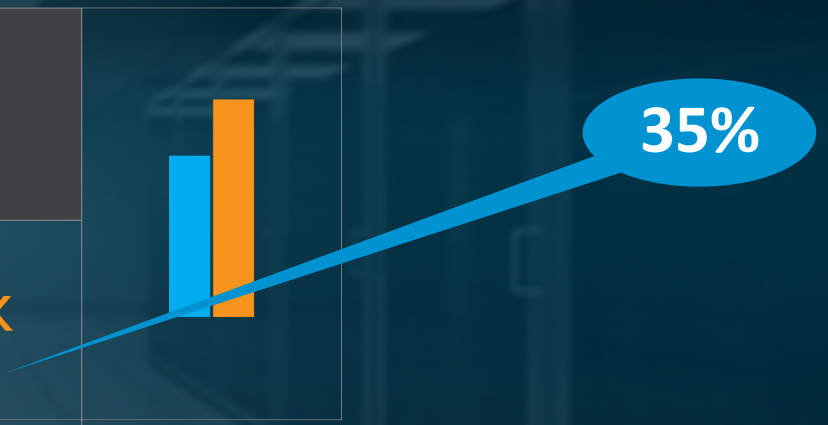
MISLEADING APP | FAKE AV | LOCKER RANSOMWARE | CRYPTO RANSOMWARE




2016 Internet Security Threat Report Volume 21

# 35% Increase in Crypto-Ransomware Attacks

| Crypto-Ransomware Total | |
|---|---|
| 2014 | 2015 |
| 269K | 362K |
| – | +35% |
| Average Per Day | Average Per Day |
| 737 | 992 |

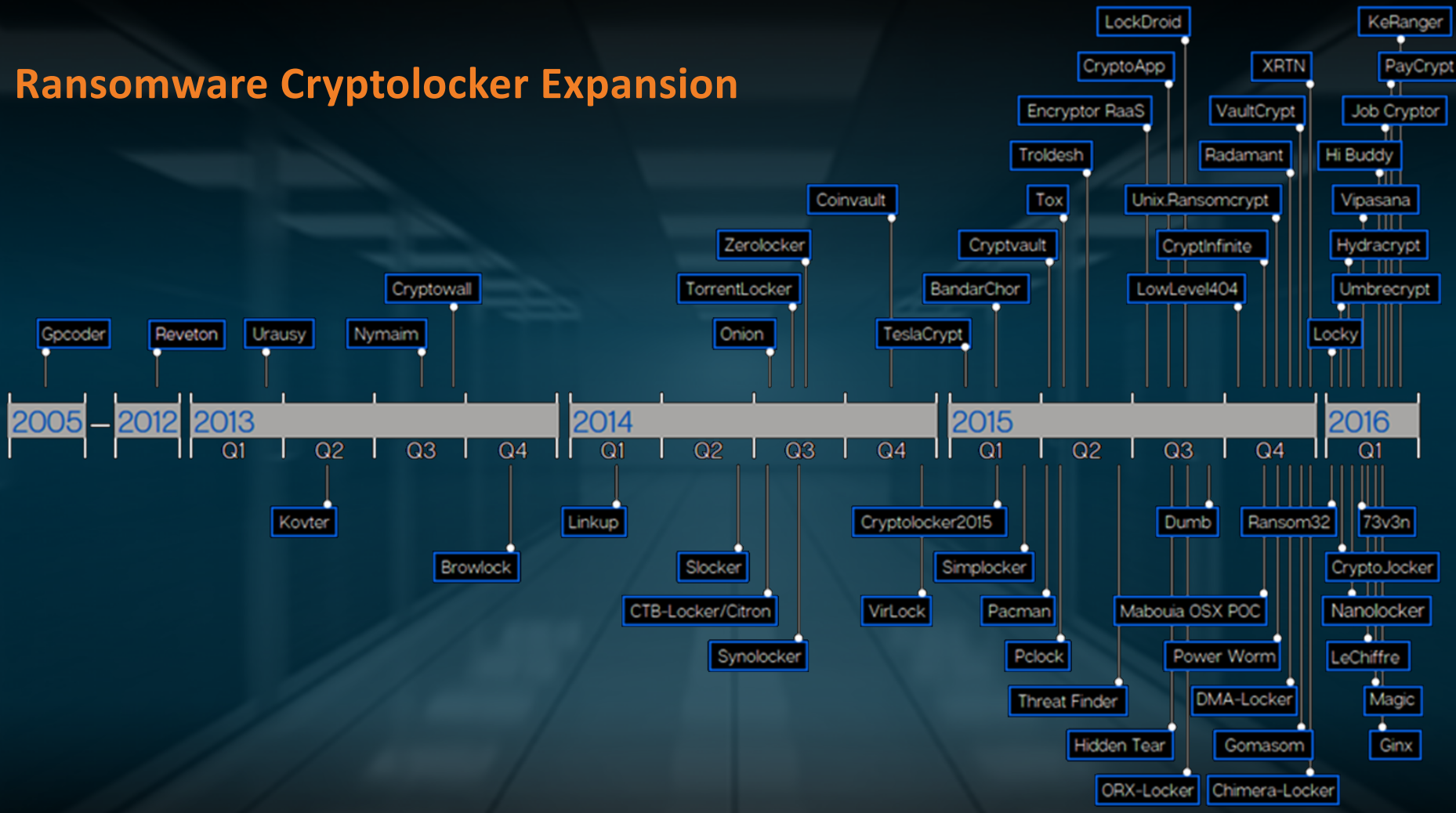


# Growth factors

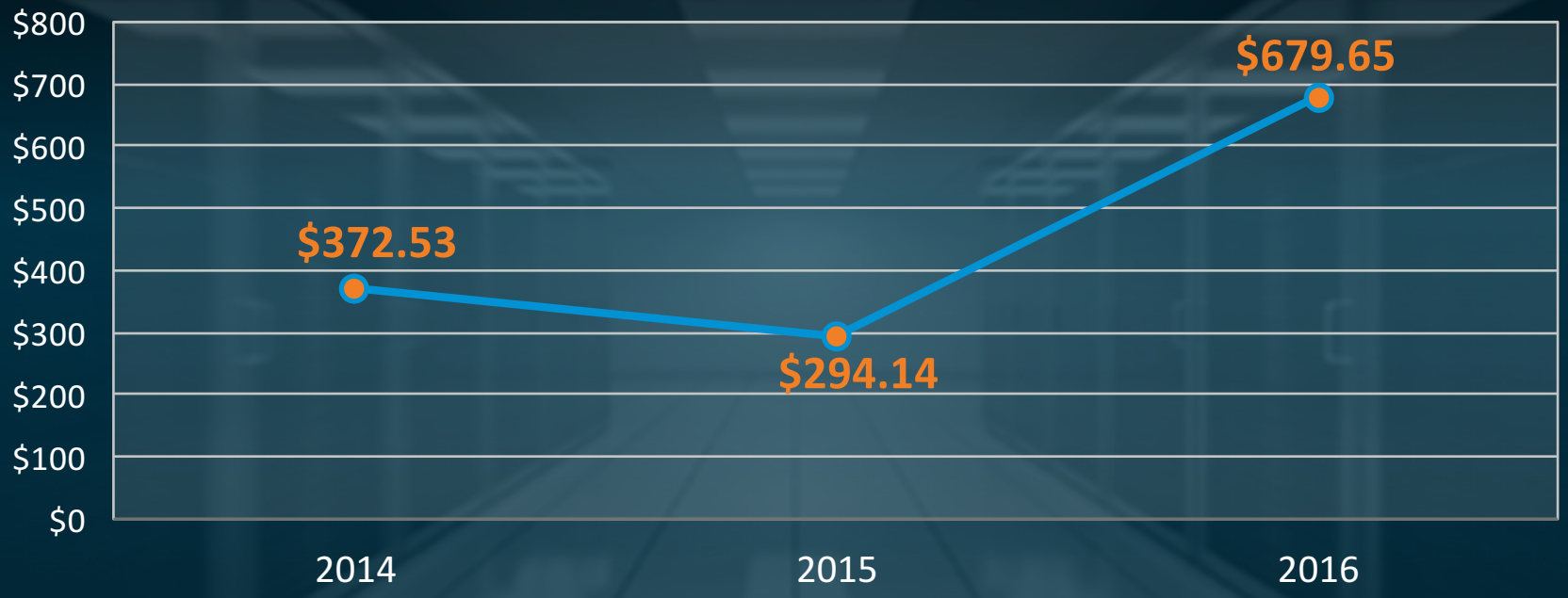
- Still profitable for the attacker
- Easy access to encryption
- Cryptocurrencies
- Effective infection vectors
- Adoption of advanced attack techniques
- Ransomware as a service

**100 new families** identified in 2015 compared to 77 in 2014
79 new families in 2016 so far

# Ransomware Cryptolocker Expansion



# Ransom demand increased




Average ransom demand has more than doubled

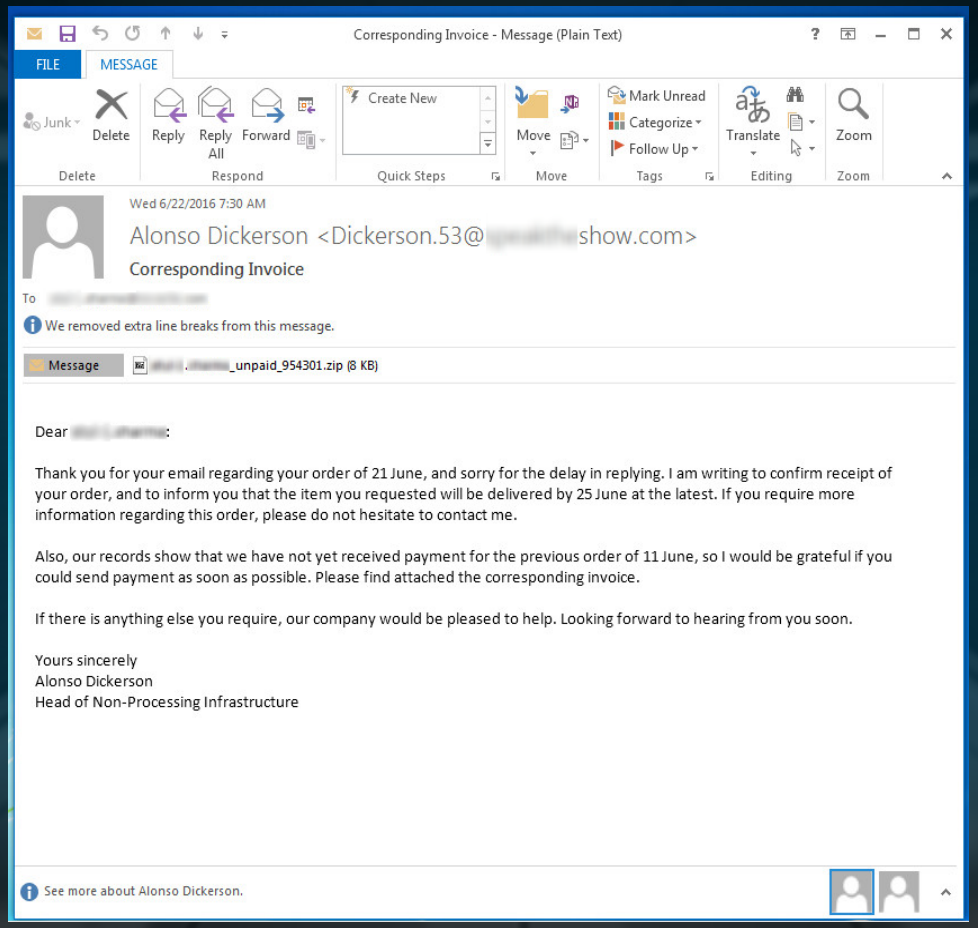
# Common infection methods

- **Email**
  - Script file (Javascript, VBS, Powershell,…)
    - Can be in archives (Zip, RAR, HTA, WSF,…)
  - Office with malicious macro (and social engineering)
  - Link to malicious files on Dropbox & Co.

- **Infected Websites**
  - Web exploit toolkits
  - Malvertisement

- **Targeted**
  - Server exploits (e.g. Jboss)
  - Bruteforcing passwords (e.g. RDP)

# Example of Spam Email Distributing Locky



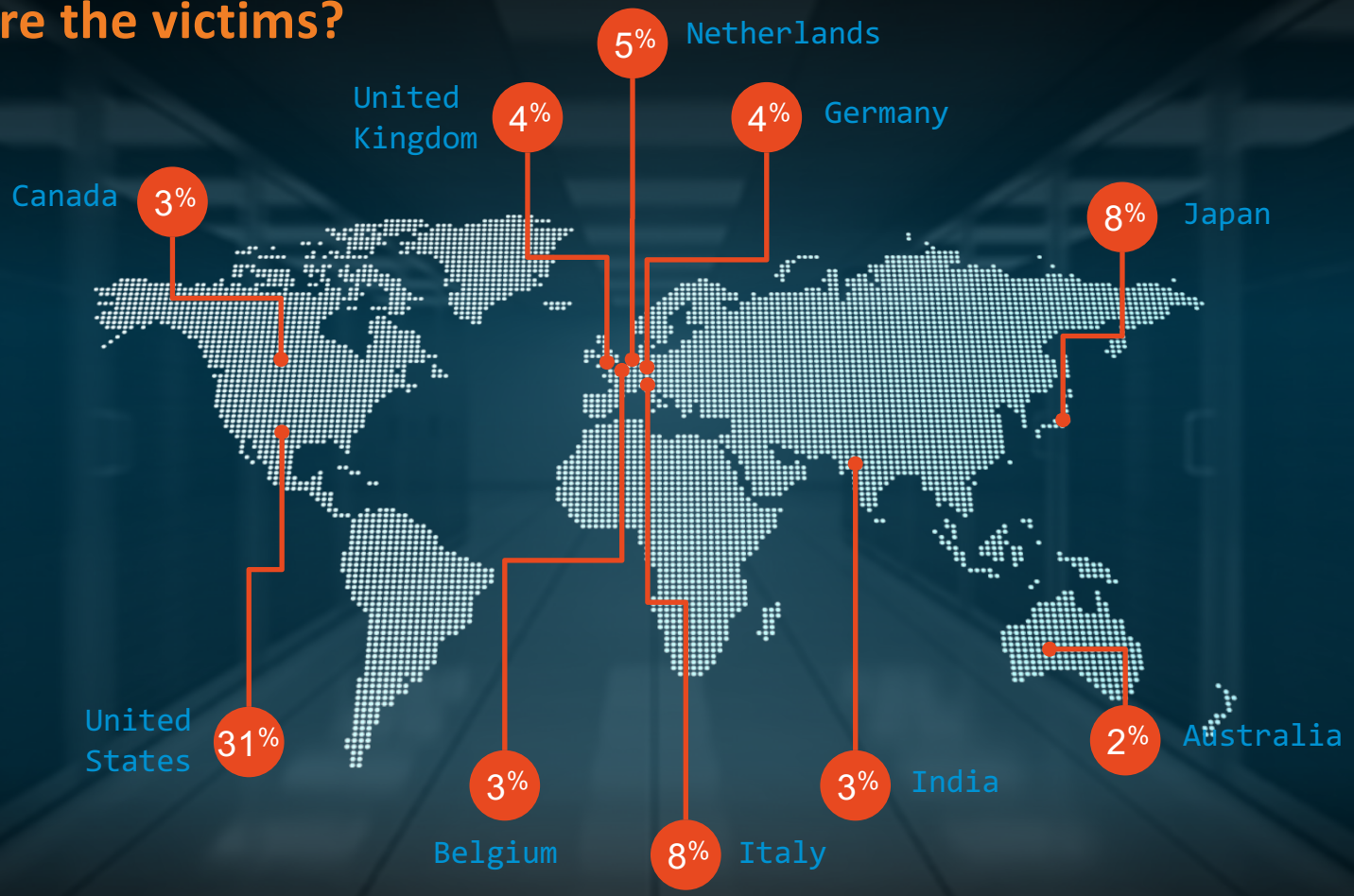
# Typical Locky Ransom Note

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. [redacted]
2. [redacted]
3. [redacted]
4. [redacted]

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

# Where are the victims?



# Businesses as a target

- Cybercrime is not just an end-user problem
- 43% of ransomware infections occur inside business
- Organizations are being targeted APT's
- User behavior is being leveraged criminally
- All Segments & Verticals are Affected

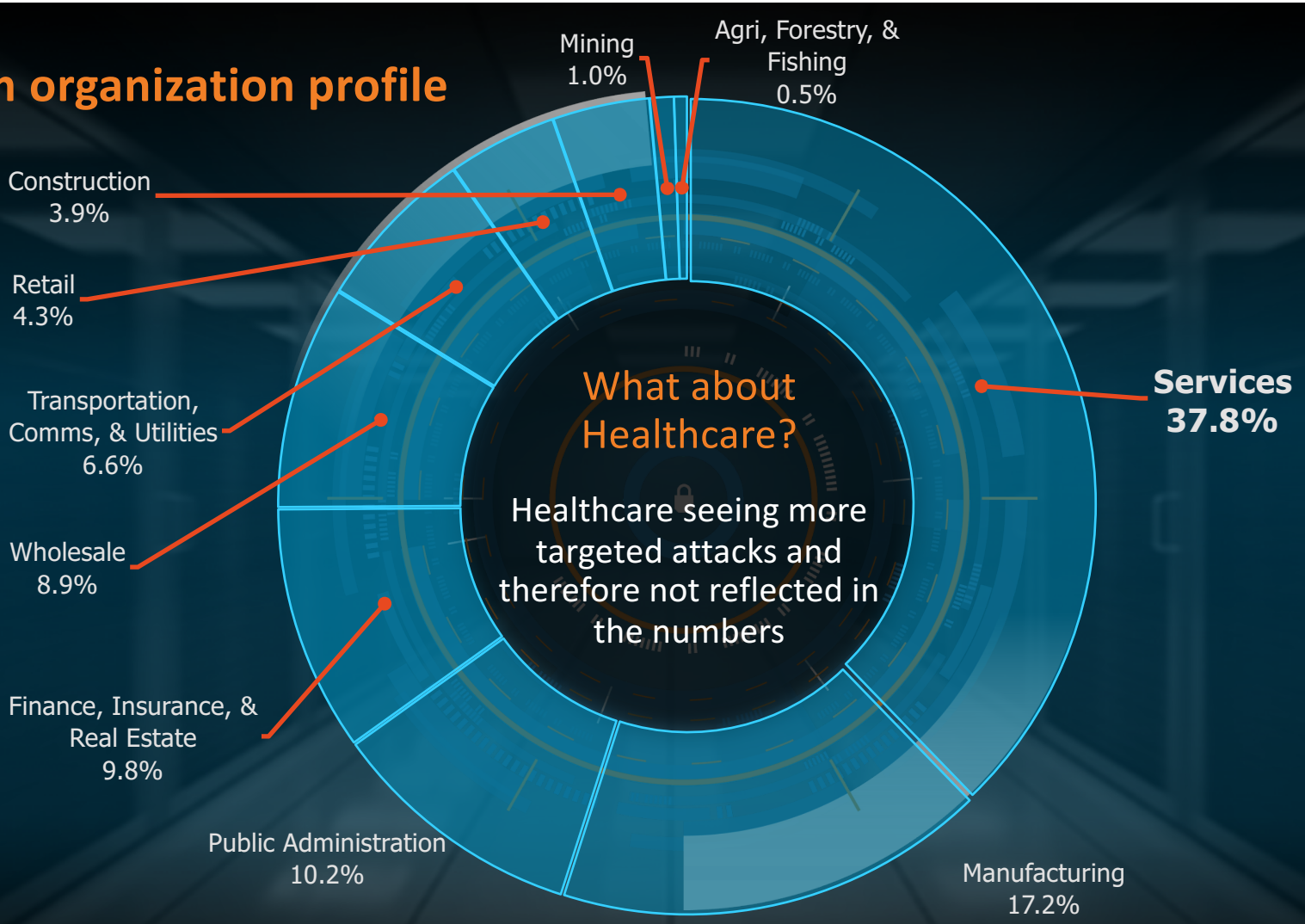
# Advanced attack techniques

Recent ransomware attacks use tactics and techniques typically seen in APT-style attacks

| | |
|---|---|
| **Infiltration** | Exploit server-side vulnerabilities to gain access to the network. |
| **Reconnaissance** | Attackers gather information that may help in later stages of the attack, such as back-up policy. Information gathered may also be used in the ransom note. |
| **Lateral movement** | Attackers use publicly available tools to plot out and traverse the network and gain access to strategic locations. |
| **Stealth** | Once the attack has been successfully carried out the attackers attempt to hide their tracks by removing any tools used. |

TLP:GREEN

# Victim organization profile



# Ransomware-as-a-service

10-09-2016, 11:03 AM

**AtomProject**
Member

Join Date: 10-09-2016
Posts: 1
Deposit account $: 0

**Atom Affiliate Ransomware Program (Cryptolocker)**

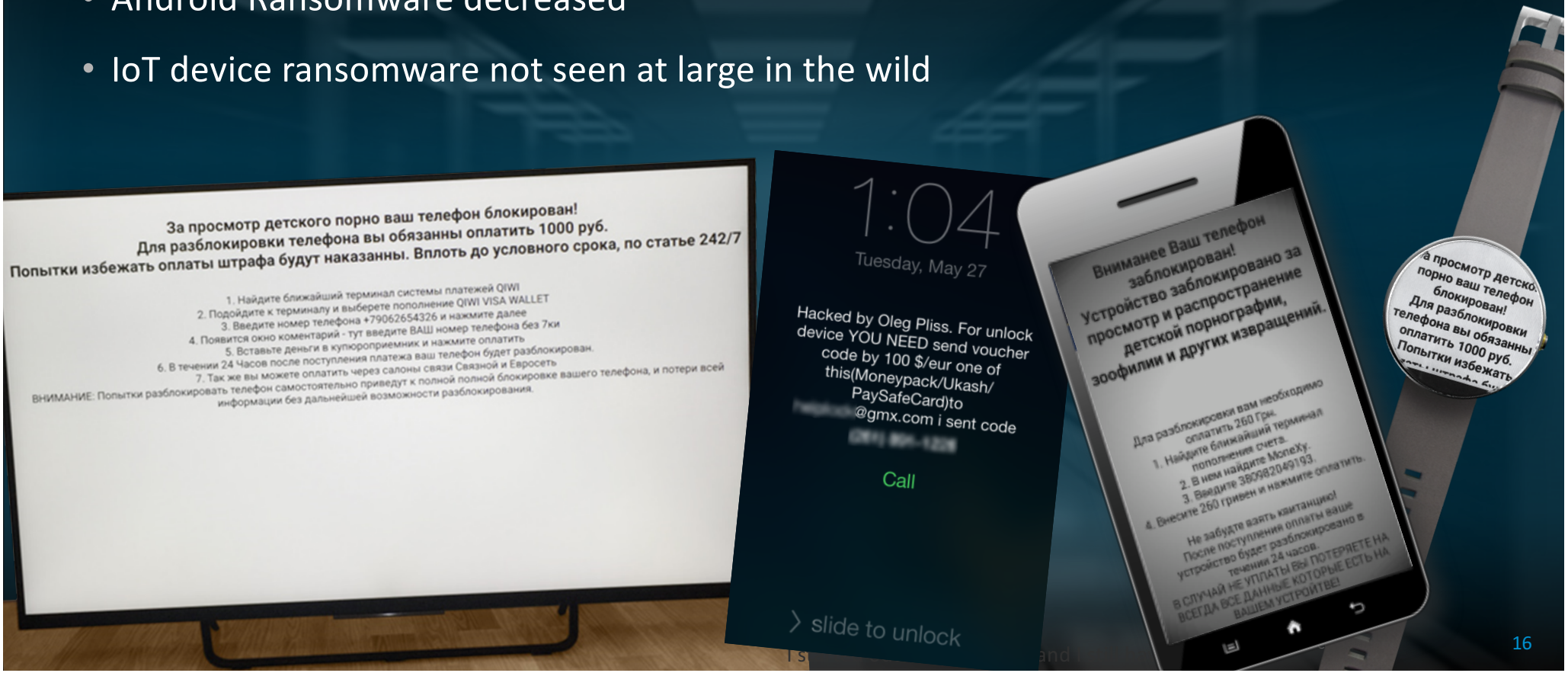
Hello, I would like to introduce you to the new ransomware affiliate program:
Description:
1. Fully Customizable (You can choose file formats and price for your attack)
2. Fully Translated (The program supports multiple languages)
3. Fully Automated (Receiving payments is fully automated)
4. Fast Algorithm (It uses a fast and reliable encryption algorithm)
5. Monetization (You will receive 80% of the payment amount directly to your Bitcoin wallet)
6. Undetectable by AV (Every day we change the source code, to avoid the appearance in anti-virus databases)
7. Tracking System (You can see online statistics of your payload)

More info: atomproject.ml
Contact Us: BM-2cUFsjnxNmjxyEpqiT2nu3AF4juyjAym6v@bitmessage.ch

Attention!
I recommend you to run all tools inside virtual machine.
(Previous project: SharkRansomware)

# Ransomware on Smart Devices

- Android Ransomware decreased
- IoT device ransomware not seen at large in the wild

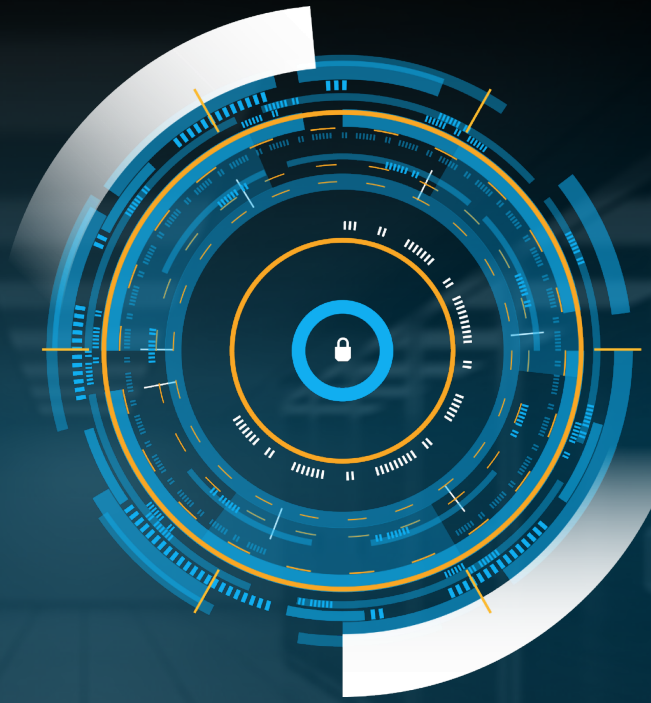


TLP:GREEN

ISTR

Internet Security Threat Report

# Thank you!




**Bill Wright**

Director, Government Affairs & Senior Policy Counsel