Ransomware Prevention and Recovery Checklists

Presented by

Tony Fondo, ISM
Northwest Regional Data Center
40% of the businesses surveyed have suffered at least one ransomware attack in the past year.

34% of those businesses lost revenue as a result of ransomware attacks.

20% of the businesses surveyed “have had to stop operations entirely in the aftermath of a successful data breach.”

60% of enterprise ransomware attacks each demanded a ransom of more than $1,000, and 20 percent demanded more than $10,000 each. Some ransom demands reported by survey respondents exceeded $150,000.

63% of respondents said it took more than a full business day to install patches and “fix vulnerable endpoints” after a successful attack.
According to a June 2016 survey from Osterman Research, almost one out of every two participants indicated their organization had suffered an at least one ransomware attack in the past 12 months. In addition, just four percent of respondents from U.S. organizations said they were very confident in their current security’s ability to prevent a future attack.
56,000 ransomware infections in March 2016, alone

Throughout the majority of 2015, the average number of ransomware infections fluctuated between 23,000 and 35,000 per month, according to Symantec. The spike to 56,000 in March 2016 coincided with the arrival of Locky, distributed primarily by the Necurs botnet, one of the largest networks of infected computers in the world.

Source: Symantec
Prior to an attack, 4 out of 5 organizations are confident backup can provide them with complete recovery

Source: Barkly

In a survey we conducted with IT pros from over 300 organizations, nearly 100% reported they were actively backing up their data. Out of those who had not yet experienced a ransomware attack, 81 percent said they were confident they would be able to recover any data attackers encrypted from backup, without paying the ransom.

Less than half of ransomware victims fully recover their data, even with backup

Source: Barkly

Of the IT pros we surveyed who had experienced a ransomware attack, only 42 percent reported being able to successfully recover all their data from backup. Common reasons for incomplete backup recovery included unmonitored and failed backups, loss of accessible backup drives that were also encrypted, and loss of between 1-24 hours of data from the last incremental backup snapshot.
Despite several high-profile examples of organizations willing to pay the ransom to recover their data, plus advice from the FBI recommending as much (at least until they revised their stance in late April), the overwhelming majority of the IT pros we surveyed said they have never and would never consider paying the ransom.

Not only did many consider it a matter of principle, there was also a healthy dose of skepticism that paying would actually result in them getting their data back. As Kansas Heart Hospital learned the hard way in May, criminals don’t always follow through with their promises to decrypt the data.

Only 5 percent ever consider paying the ransom an option

Source: Barkly

Your personal files are encrypted!

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open http://maktubuyatq4rfyo.onion.link
or http://maktubuyatq4rfyo.torstorm.org
or http://maktubuyatq4rfyo.tor2web.org
Email is the #1 delivery vehicle for ransomware

Emails with malicious links and malicious attachments account for 59 percent of ransomware infections. According to the Osterman Research survey, users are more than twice as likely to be infected by clicking something in an email than visiting an infected website directly. Big takeaway: Don’t click it, no support ticket.
7 out of 10 malicious email attachments delivered Locky in Q2 2016

Source: Proofpoint

If one of your users got their files encrypted after opening a malicious email attachment in Q2, chances are it was Locky. Typically hidden in MS Word documents and executed by leveraging macros, Locky has quickly become one of the most prevalent ransomware families out there. It’s almost exclusively distributed via spam email campaigns powered by the Necurs botnet (notorious for also distributing the Dridex banking trojan).
Nearly two-thirds of exploit kits have ransomware payloads

Phishing emails may be the top delivery vehicle for ransomware, but exploit kits are dropping their fair share of the stuff, too. In fact, in just five months (from December 2015 to May 2016), ransomware jumped from being included in just 17 percent of exploit kits to being the most popular payload by far.

Source: Malwarebytes
That said, exploit kit traffic has plummeted since the disappearance of the Angler EK in early June. Up to that point, Angler had been the dominant exploit kit (accounting for 60 percent of total EK traffic). In its absence, exploit kits like Neutrino and RIG are now vying to slowly fill the vacuum.
In June 2016 we surveyed 1,138 companies in a variety of industries and compared the levels of concern about ransomware in 2014 to 2016. It's not a pretty picture.

- Actual Infections practically doubled from 20% to 38%
- 61% feel email attachments pose the largest threat
- Nearly half say they would be forced to pay the ransom if backups failed
- Confidence in filters is only 72%
- 88% feel security awareness training is the most effective protection from ransomware over 83% for backup, almost identical to 2014

*SOURCE: BeyondTRUST*
Typical ransomware software uses RSA 2048 encryption to encrypt files. Just to give you an idea of how strong this is, an average desktop computer is estimated to take around 6.4 quadrillion years to crack an RSA 2048 key.

One estimate indicates more than $27 million in ransom payments in just the first few months of the release of the CryptoLocker variant of ransomware in September 2013.

CryptoLocker was followed up by the variant CryptoWall, which made $325 million dollars in 18 months, half of that in the United States. By now there are thousands of ransomware victims, including a New Jersey School District, police departments in Maine, Massachusetts & Chicago.
Heads-up! Individual ransomware payments are getting very expensive. Companies are stockpiling Bitcoin in case they are hit, and a new low-profile strain of ransomware called Crysis is actually causing a data breach. If you need more IT security budget, this is the most powerful ammo seen. Here are the highlights:

• Health Center Paid 68 Bitcoins (40K) To Get 250 Machines Back.
• University Pays Hackers 20,000 Dollars To Get Back Its Infected Files.
• Hackers Hold A School District Hostage For Almost 10,000 Dollars.
• Companies Are Stockpiling Bitcoin In Case They Get Infected With Ransomware.
• Worst Of All, Low-Profile Crysis Ransomware Is Actually Causing A Data Breach.

SOURCE: BeyondTRUST
Your files are encrypted.
You did not pay in time for decryption, that's why the decryption price increases 2 times. At the moment, the cost of decrypting your files is 1000 USD/EUR. In case of failure to 25/05/14 - 11:44 your key will be deleted permanently and it will be impossible to decrypt your files.

Your system: Windows 7 (64)  First connect IP: 123.45.67.89  Total encrypted 4 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 everyday.
   - How To Buy Bitcoins - An international directory of bitcoin exchanges.
   - Cash Into Coins - Recommended for fast, simple service.
   - Coinbase - Bitcoin exchange based in the United States. (Highly rated).
   - BitStamp - A multi-currency bitcoin exchange based in Slovenia. (Highly rated).
   - CoinJar - CoinJar allows direct bitcoin purchases on their site. They're based in Australia but serve an international clientele.
3. Send 2.44 BTC to Bitcoin address: [Redacted]
4. Enter the Transaction ID and select amount:
   - 2.44 BTC = 1000 USD
   - [Clear]
   - Note: Transaction ID - you can find in detailed info about transaction you made (example: 44214d3a56e5f5f5836c6d209d0f3e483f1127e4d2f070b3e2a2388146d4f12)
5. Please check the payment information and click "PAY".

Thank you.

JIGSAW RANSOMWARE

Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.

If you do not have bitcoins Google the website localbitcoins. Purchase 150 American Dollars worth of bitcoins or .4 BTC. The system will accept either one. Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryption key and return.
Try anything funny and the computer has several safety measures to delete your files.
As soon as the payment is received the encrypted files will be returned to normal.

Data Center
NWRDC

Spyware.com
Some quick facts about Bitcoins:
- Bitcoins are commonly abbreviated as BTC, and are untraceable.
- The price of Bitcoins is constantly fluctuating. At the time of this writing 1 BTC is roughly $400.
- You can buy partial Bitcoins. For example, you can buy 0.5 BTC (half of a Bitcoin). An individual Bitcoin can be split in up to many extremely small fractions.
- There will only ever be 21 Million Bitcoins in circulation once they are all available.

A few facts about TOR:
- Instead of using .com or .net domains, onion web addresses end in .onion.
- You cannot browse TOR sites using a regular Internet browser.
- TOR was originally developed by the U.S. Naval Research Laboratory and Defense Advanced Research Projects Agency (DARPA).
Thanks!