Abstract

With spring comes the blossom of DDoS for Ransom (RDoS) attacks. In 2016, ransom was the #1 motivation behind cyber-attacks; half of organizations were subject to this extortion threat (according to Radware's *2016-2017 Global Application & Network Security Report*). In parallel to the ransomware plague, Radware witnessed an emerging trend of hackers (and copycats) who extort organizations by posing an imminent threat of a DDoS attack – one out of six organizations was a victim. As IoT botnets have become more powerful, Radware has witnessed an increase in the number of ransom threats that companies have received in 2017. So far, two hacker groups have risen above the rest: XMR Squad and FancyBear.

RDoS in 2017

In an RDoS attack, the perpetrators send a letter threatening to attack an organization—rendering its business, operations or capability unavailable—unless a ransom is paid by the deadline. These attacks have grown in number every year since 2010 and typically come in the form of a volumetric distributed denial of service (DDoS) attack. However, it is increasingly in vogue to find techniques that are more piercing and more efficient without generating large volumes. The most advanced attacks combine both volumetric and non-volumetric cyber-attack techniques.

RDoS ROI

RDoS has become financially rewarding to cyber criminals who enjoy large monetary gains for very small investments. For example – opening a bitcoin wallet and sending an extortion email costs nearly nothing. Distributing enough ransom letters will usually generate a few individuals/organizations that are willing to pay. Moreover, hackers increase their chances by paying as little as $20 for a DDoS-as-a-service program and launch a twenty-minute 1 Gbps-demo attack. The reward, in most cases, is thousands of dollars. For this reason, there have been many opportunists that emerged in 2016, such as the hacktivist group that tried to use the name of the infamous group Lizard Squad to spread fear and extort victims. This year it is a group pretending to be Fancy Bear/APT28.

How to tell whether an RDoS threat is real?

FancyBear

At the end of April, FancyBear began sending out extortion attempts. The extortionist behind this campaign attempted to intimidate their victims by using APT28, a cyber-espionage group. APT28 is a nation state-level attacker that uses zero-day exploits and spear phishing attacks to spread their malware. RDoS campaigns are not FancyBears' modus operandi.

```
FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are the Fancy Bear: https://fancybear.net
All your servers will be DDOS-ed starting Friday (April 28) if you don't pay protection - 10 Bitcoins @


If you don't pay by Friday, attack will start. The fee will increase by 10 Bitcoins for each day that
has passed without payment.

Our attacks are extremely powerful - sometimes over 1 Tbps per second.
So, no cheap protection will help.
Prevent it all with just 10 BTC @

There's no counter measure to this, you will only end up wasting more money trying to find a solution.
We will make sure your website will remain offline until you pay.
This is not a hoax. Once you have paid we won't start attack AND YOU WILL NEVER AGAIN HEAR FROM US!
Please note that Bitcoin is anonymous and no one will find out that you have complied.
```

Figure 1: Ransom note from FancyBear

The wording of the extortion attempt was similar to a fake Armada Collective letter from last year[i]. FancyBear was requesting 10 bitcoins with the threat to increase by 10 bitcoins for each day without payment. Unlike genuine RDoS attackers, FancyBear did not launch a demonstration attack. Demonstration attacks prove that a threat is real. Ultimately, FancyBear never launched an attack. Their main objective was to leverage the name of a well-known threat to force the victim into paying the ransom.

XMR Squad

Radware's ERT research is also monitoring[ii] another RDoS campaign in parallel. This new group, XMR Squad, has already targeted companies in Germany and the United States. Companies in Germany included DHL, Hermes, AldiTalk, Freenet and Snipes.com. The attack launched against DHL by XMR Squad shut down their customer portal and all API services.

XMR Squad, unlike FancyBear, launched attacks against their victims. After launching a demonstration attack, XMR Squad emailed their victims requesting 250 Euros for testing their DDoS mitigation systems. Currently, a different group going by the name XMR Squad is requesting 2-3 bitcoins under the threat of a 300 - 600 Gbps attack. The time limit given for payment is 24 hours.

Figure 2: @XMR_Squad

XMR Squad disappeared about one week ago but has since reappeared. The unusual part about XMR Squad is the way they went about branding and marketing themselves. They have a Twitter account, @XMR_Squad, a website, xmr-squad.biz, and did an interview. Notorious RDoS groups like DD4BC and Armada Collective did not have a website or Twitter accounts.

It's likely that XMR went public during their original campaign so they could establish a name for themselves. When they come back, they would have an established reputation of launching attacks. The problem is the latest group to claim they are XMR Squad has not followed through with their threats. Radware has witnessed a number of extortion letters over the last several days, but the extortionist has not launched an attack. The new XMR Squad has also switched from requesting Euros to bitcoin. They are requesting payment with no demonstration attack and no follow through.

```
FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are xmr-squad. https://lmgtfy.com/q=xmr_squad

All your servers will be DDoS-ed starting starting (may 2) if you don't pay protection - 2 Bitcoins @

If you don't pay by tuesday, attack will start, price to stop will
increase to 20 BTC and will go up 5 BTC for every day of attack.

One bitcoin costs about 1.3k USD at the moment.
You can buy bitcoins easily here: https://blockchain.info/wallet

This is not a joke.
Our attacks are extremely powerful - sometimes over 300 Gigabits per second.
So, no cheap protection will help.

Prevent it all with just 2 BTC @

Do not reply, we will not read.
Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.
```

Figure 3: Ransom letter sent by XMR Squad on May 1, 2017

Attack Vectors

Most of these DDoS for ransom groups are running their own network stressers, however some leverage publicly-available stressers to conduct their campaigns. When experiencing a DDoS for ransom attack, expect 100+ Gbps and multi-vector attacks simultaneously. The attack is likely to be persistent and last for days. Attack vectors include floods using the following protocols:

- SSDP
- NTP
- DNS
- UDP
- TCP RST
- TCP SYN
- SYN Flood
- SYN ACK
- SSYN
- ICMP

RDoS Groups

- DD4BC
- Armada Collective
- RedDoor
- exBTC
- Kadyrovtsy
- Borya Collective
- Lizard Squad (fake)
- Stealth Ravens
- XMR Squad
- FancyBear

Dealing With a Ransom Letter

Companies should be advised not to pay an extortionist and seek professional assistance with mitigating an RDoS attack. Such a threat usually provokes the need for a scrubbing service, ACL/BGP reconfiguration, as well as the usual DDoS protection essentials (listed below) to assure uptime and SLA.

Evaluation - Is It Real or Fake?

Although it is almost impossible to determine whether a ransom note comes from a competent, experienced hacker group or an amateur unit - some units emerged under the guise of notorious hacking crews. While these fake groups send emails nearly identical to real ransom letters, there are several indicators to distinguish between the two:

1. The fake groups often request a different amount of money.
2. "Real" groups prove their competence; fake groups exclude the "demo" attack.
3. These groups do not have official accounts, websites or target lists.
4. When hackers launch a real ransom attack, they normally target many companies under the same industry.
5. Look for suspicious indicators. Is this group known for DDoS attacks?

Organizations Under Attack Should Consider

- **Hybrid DDoS Protection** - (on-premise + cloud) – for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - to quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - to promptly protect from unknown threats and 0-day attacks
- **A Cyber-Security Emergency Response Plan** - that includes a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

For further security measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button".

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

---

[i] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/ransom-attacks/
[ii] https://www.bleepingcomputer.com/news/security/xmr-squad-is-charging-german-companies-250-for-ddos-tests-/