S-RM

AUGUST 2018

‘WE’RE BACK, YOU CLOWNS’:

How to respond to a Hacking Threat

BUSINESS INTELLIGENCE I CRISIS MANAGEMENT I CYBER SECURITY

‘WE’RE BACK, YOU CLOWNS’:

How to respond to a Hacking Threat

James Jackson from S-RM Cyber Security investigates the series of attacks on ProtonMail to pull out some valuable lessons on what motivates various threat actors and how you can respond when you’re in the crosshairs.

Most people have never met a hacker. Your organisation probably has. Every day, a vast range of individuals and groups probe the world’s networks and security systems. Whilst for the majority of the time this is to little effect, when there is a serious incident, suddenly you may find yourself personally managing the response to this new adversary.

The following story gives some insight into how to react when this happens. It also demonstrates how interrogating the identities, motivations, and capabilities of these threat actors can dramatically improve your ability to respond to a crisis.

Back in 2015, the Swiss-based encrypted email platform ProtonMail, just a year into operations, suffered a devastating Distributed Denial of Service (DDoS) event that continues to resonate throughout the security industry.

It all started in the middle of the night on 4 November, when CEO Andy Yen received a ransom note demanding 15 Bitcoins, which was around EUR 6,500 (back then – how times change), or else the company would be the latest target of a hostile group of cyber criminals wanting to test their abilities. They didn’t pay, and less than 12 hours later these attackers, calling themselves Armada Collective, started flooding them with data – sending their website offline.

For several hours, ProtonMail tried and failed to repel the unrelenting attack. After appealing to industry experts and working with local government agencies, they soon discovered a worrying dynamic - the attacks were becoming increasingly sophisticated, and the impact was rapidly spreading to other businesses. This was now one of the largest recorded DDoS attacks seen in Europe, reaching up to 100Gbps. The sophistication of the attackers meant that they had begun targeting the infrastructure ProtonMail were sharing with other businesses, reportedly disrupting over 100 firms, some of which were hosting mission critical services. Faced with a swarm of angry businesses, ProtonMail agreed to pay the ransom.

Despite this, the attacks didn’t stop. Worryingly, Armada Collective issued a communication swearing that they had received the ransom and had stopped their attacks, and yet the onslaught continued. There was a second threat actor in play. This is now understood to be a state-sponsored group. They had effectively piggybacked onto the operation and used it as a cloak to hide their own attacks.

Eventually, having been forced to create a crowdfunding campaign to help finance their response, ProtonMail managed to control the attack and appear back online. One of the first things they said was, “ProtonMail will NEVER pay another ransom”. Despite this, the company continues to face high-profile cyber threats, most recently in June this year.

WHAT CAN WE LEARN?

ProtonMail’s story is useful because it illustrates the importance of moving away from traditional incident response models and towards crisis management. When multiple attacks coincide or incidents grow beyond the level you can deal with internally, you must be prepared to play by a new set of rules.

ProtonMail knew there were state-actors who wanted to see its service taken offline. It was providing an encrypted email platform that anyone could use to protect their information. Therefore, governments with invasive spying capabilities, or those with a history of preventing freedom of speech, have a vested interest in preventing their citizens from using ProtonMail’s services. This threat actor was already on their register, but as we observed, they had trouble identifying their presence, and because of this they lacked the level of external support they needed until much later.

When faced with a state-actor, any sort of request for a ransom is likely to be a ruse designed to make the target underestimate the severity of the issue, as we saw with the NotPetya incidents. But at the other end of the scale we have Armada Collective, a group with the intentions of making money and increasing their reputation. They also targeted ProtonMail, but for different reasons, which required a different response.

Even though Armada Collective halted their attack after the ransom, ProtonMail have suffered ever since. As recently as 27 June this year, they were the target of the Apophis Squad hacker group. Whilst they did not issue a ransom, Apophis Squad wanted to leverage the popularity of attacking ProtonMail to market their new product – a tool that can DDoS other websites. For hacker groups looking to raise their profile, well-known organisations with prior public evidence of a vulnerability, or a previous record of being attacked, make very attractive targets. If you fit this description, you’re effectively an opportunity for some free PR, and your cyber posture should reflect this.

So how do you prepare for these sort of attacks? In addition to making sure you do your threat actor and capability analysis, it’s imperative that you also define a crisis response strategy. This might include building relationships with external companies or agencies that could provide support during a crisis, or just having a crisis management plan which makes sure that the right people get involved when a cyber ‘incident’ gets escalated to a ‘crisis’.

Additionally, how you interact with the public, and even the adversaries themselves, can have a significant impact. For example, in the June 27 attack, ProtonMail’s CTO Bart Butler antagonised Apophis Squad on Twitter by calling them “clowns”. In response, Apophis Squad escalated their attack and continued it over a longer period of time than they may have initially intended.

Lastly, you should always consider your general cyber security posture, and there are many ways to improve it. Most opt to adopt a set of security controls, perhaps drawing on ISO 27001 or SOC2. You don’t need to be accredited against these libraries to reap the value from using them internally. For something more active, Red Teaming is becoming increasingly popular, where a team of professional security experts attempts to compromise an organisation using a variety of digital and physical attacks.

In short, have a plan for when it happens to you.

> “In these situations, managing communication correctly is key - not just with the hackers, but internally within your organisation, and externally to law enforcement, regulatory agencies and of course the public. Each of these channels has the potential to help resolve a crisis, but can be a liability if handled inappropriately. Provoking an adversary, as we saw in this attack, is certainly ill-advised. For companies who are unfamiliar in managing these types of situations, crisis management consultants can make sure that all these different parties are liaised with at the right time to give the best chance of managing the crisis successfully.”
>
> BILL LAURENCE, DIRECTOR,
> S-RM CRISIS MANAGEMENT

S-RM IS A GLOBAL CONSULTANCY THAT HELPS CLIENTS MANAGE REGULATORY, REPUTATIONAL AND OPERATIONAL RISKS

BUSINESS INTELLIGENCE

We investigate companies and individuals on behalf of clients worldwide.

CRISIS MANAGEMENT

We help companies and individuals prevent, prepare for, and respond to crises.

CYBER SECURITY

We advise companies and individuals to ensure their data and assets are protected.

200 + employees

across 6 continents

speaking 30+ languages

supporting clients in 140 + countries

S-RM

BUSINESS INTELLIGENCE | CRISIS MANAGEMENT | CYBER SECURITY

hello@s-rminform.com | www.s-rminform.com