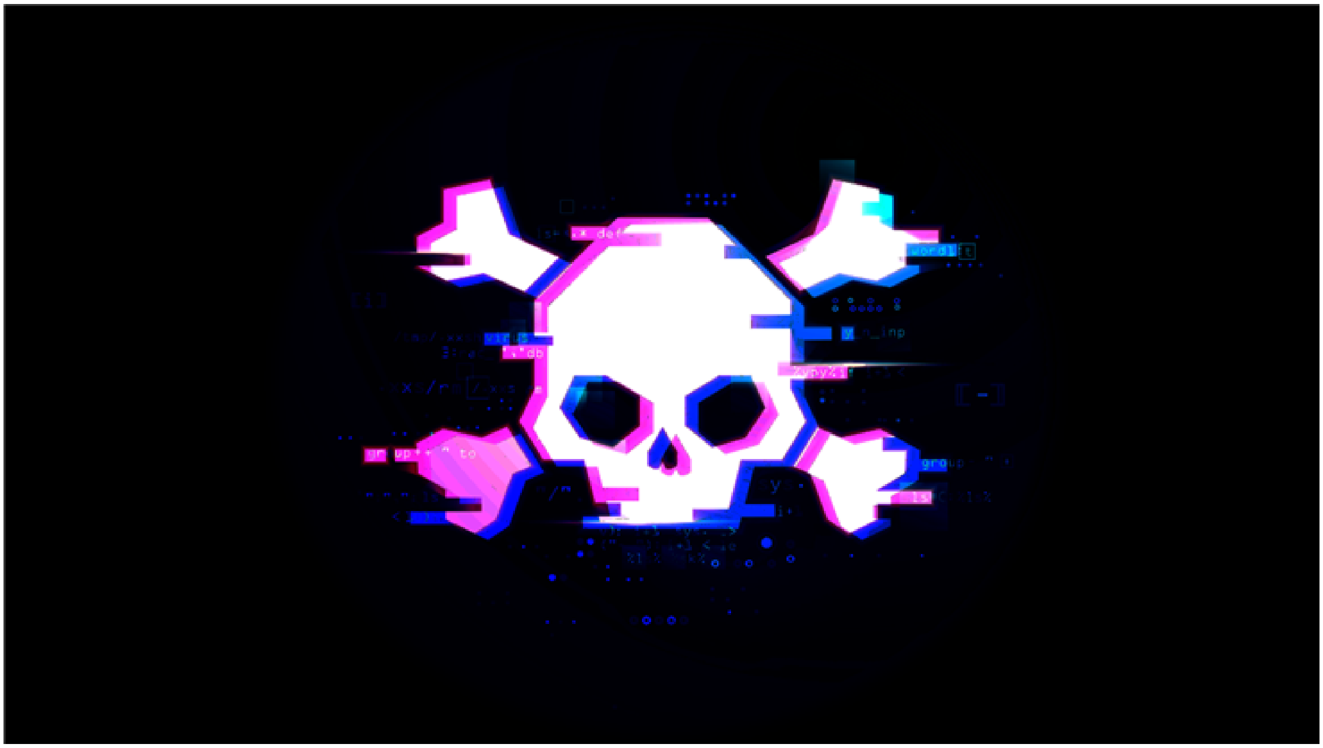
Ransomware review: March 2023

malwarebytes.com/blog/threat-intelligence/2023/03/ransomware-review-march-2023

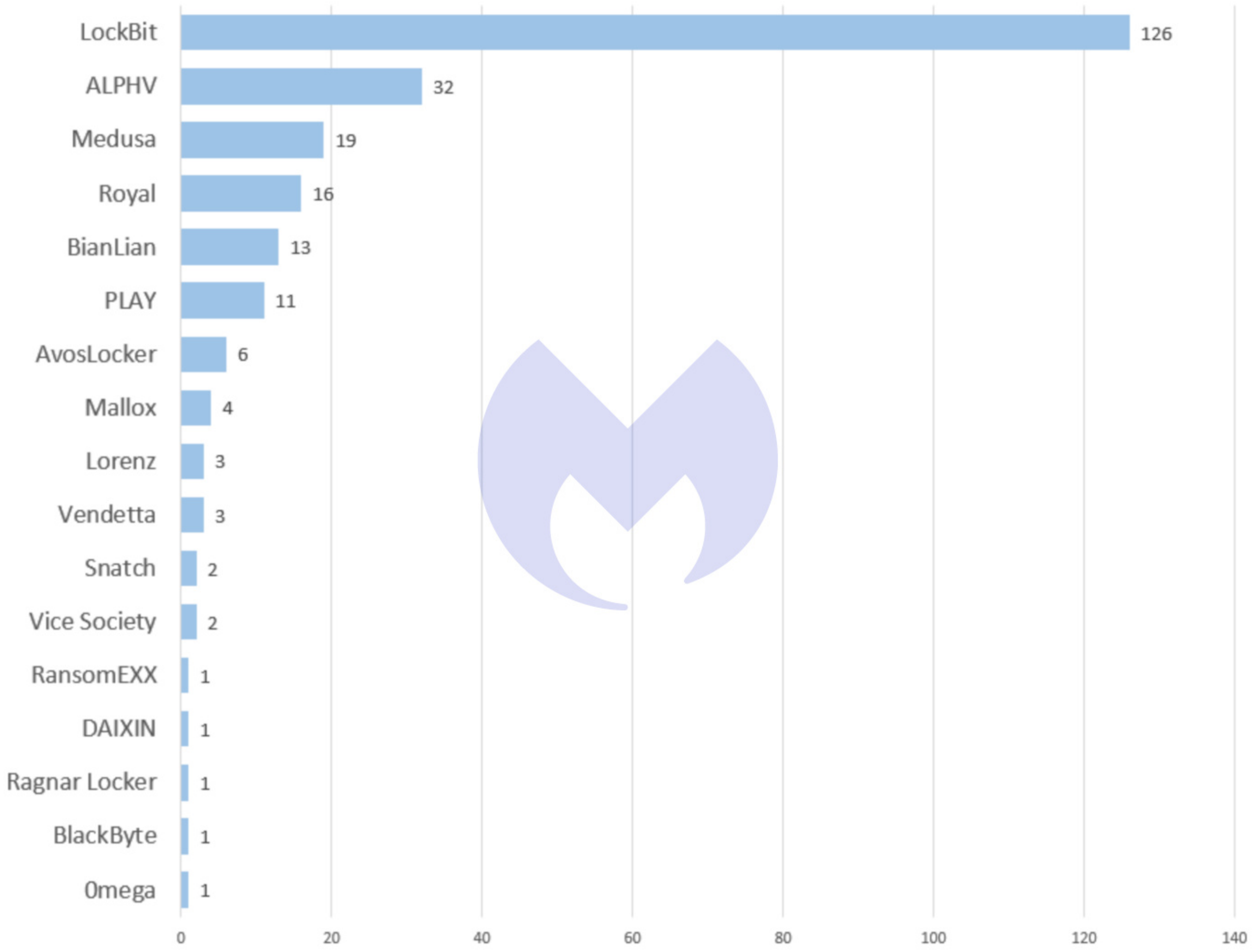


Ransomware | Threat Intelligence

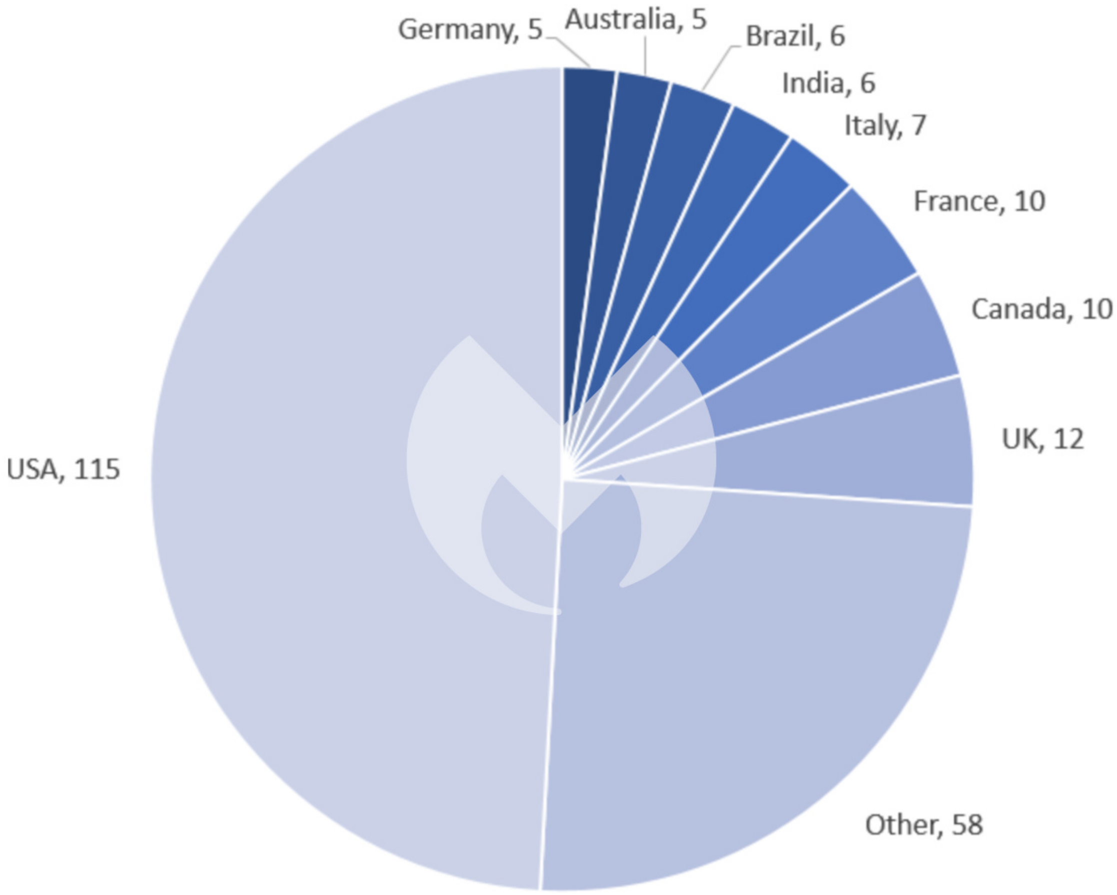
Posted: March 8, 2023 by Threat Intelligence Team

This article is based on research by Marcelo Rivero, Malwarebytes' ransomware specialist, who builds a monthly picture of ransomware activity by monitoring the information published by ransomware gangs on their Dark Web leak sites. This information represents victims who were successfully attacked but opted not to pay a ransom.

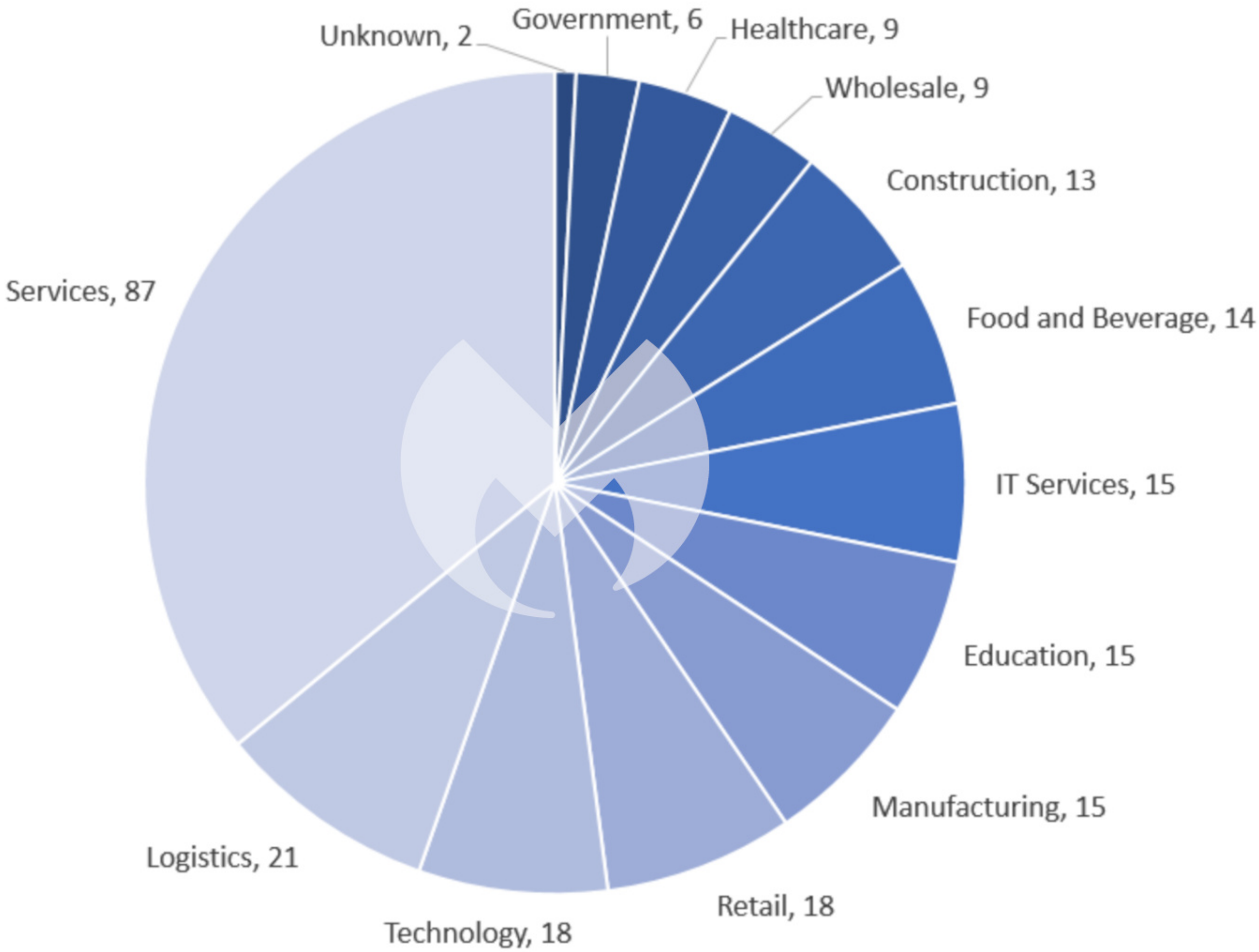
It seems like LockBit wasn't content with having us merely crown them as one of the five most serious cyberthreats facing businesses in 2023. In February, the most widely used ransomware-as-a-service (RaaS) posted a total of 126 victims on its leak site—a record high since we started tracking the leaks in February 2022.



Known ransomware attacks by gang, February 2023



Known ransomware attacks by country, February 2023

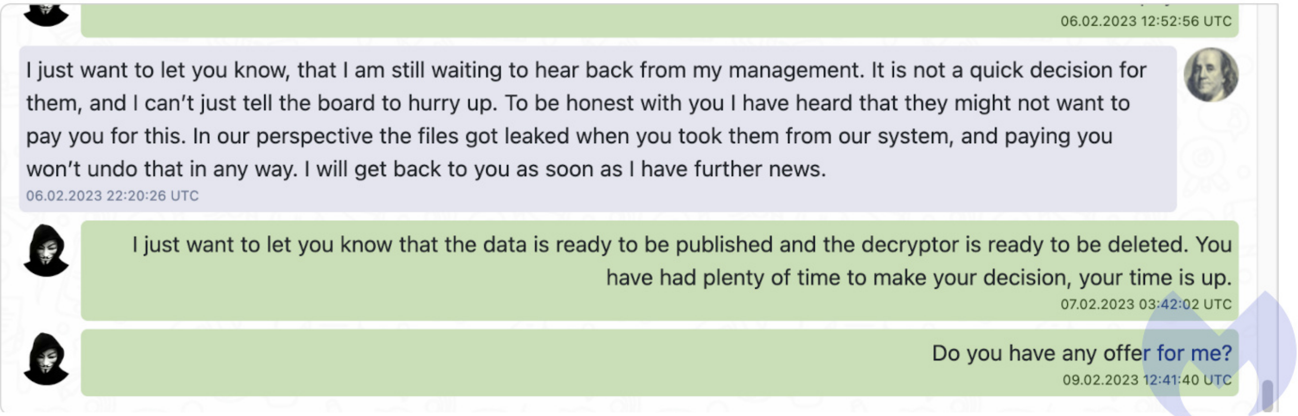


Known ransomware attacks by industry sector, February 2023

Companies attacked along LockBit’s warpath last month include financial software firm ION Group and Pierce Transit, a public transit operator in Washington state. LockBit claimed that ION Group had paid the ransom and demanded $2 million from Pierce Transit.

Speaking of ransom demands, it seems like that’s another area where LockBit broke records last month.

In early February LockBit tried to get $80 million out of the UK's Royal Mail—the largest demand since asking Continental for $50 million in 2022. Royal Mail rejected the demand, calling it ‘absurd’, and LockBit consequently published the files it stole from the company—but not without also leaking a chat history showing the negotiations between the two parties, which featured the unusual sight of a Royal Mail negotiator giving the feared ransomware gang the runaround.



06.02.2023 12:52:56 UTC

I just want to let you know, that I am still waiting to hear back from my management. It is not a quick decision for them, and I can't just tell the board to hurry up. To be honest with you I have heard that they might not want to pay you for this. In our perspective the files got leaked when you took them from our system, and paying you won't undo that in any way. I will get back to you as soon as I have further news.
06.02.2023 22:20:26 UTC

I just want to let you know that the data is ready to be published and the decryptor is ready to be deleted. You have had plenty of time to make your decision, your time is up.
07.02.2023 03:42:02 UTC

Do you have any offer for me?
09.02.2023 12:41:40 UTC

Lockbit and Royal Mail negotiations

Confirmed attacks by Vice Society, the ransomware gang infamous for wreaking havoc on the education sector, reached their three-month low last month. The apparently Russian-based group tallied just two victims on its leak site in February, but—true to their modus operandi—both of them were educational institutions: Guildford County School, a specialist music academy in London, and Mount Saint Mary College, a liberal arts college in New York. Needless to say, we're not banking on this persistent education sector threat going away anytime soon.

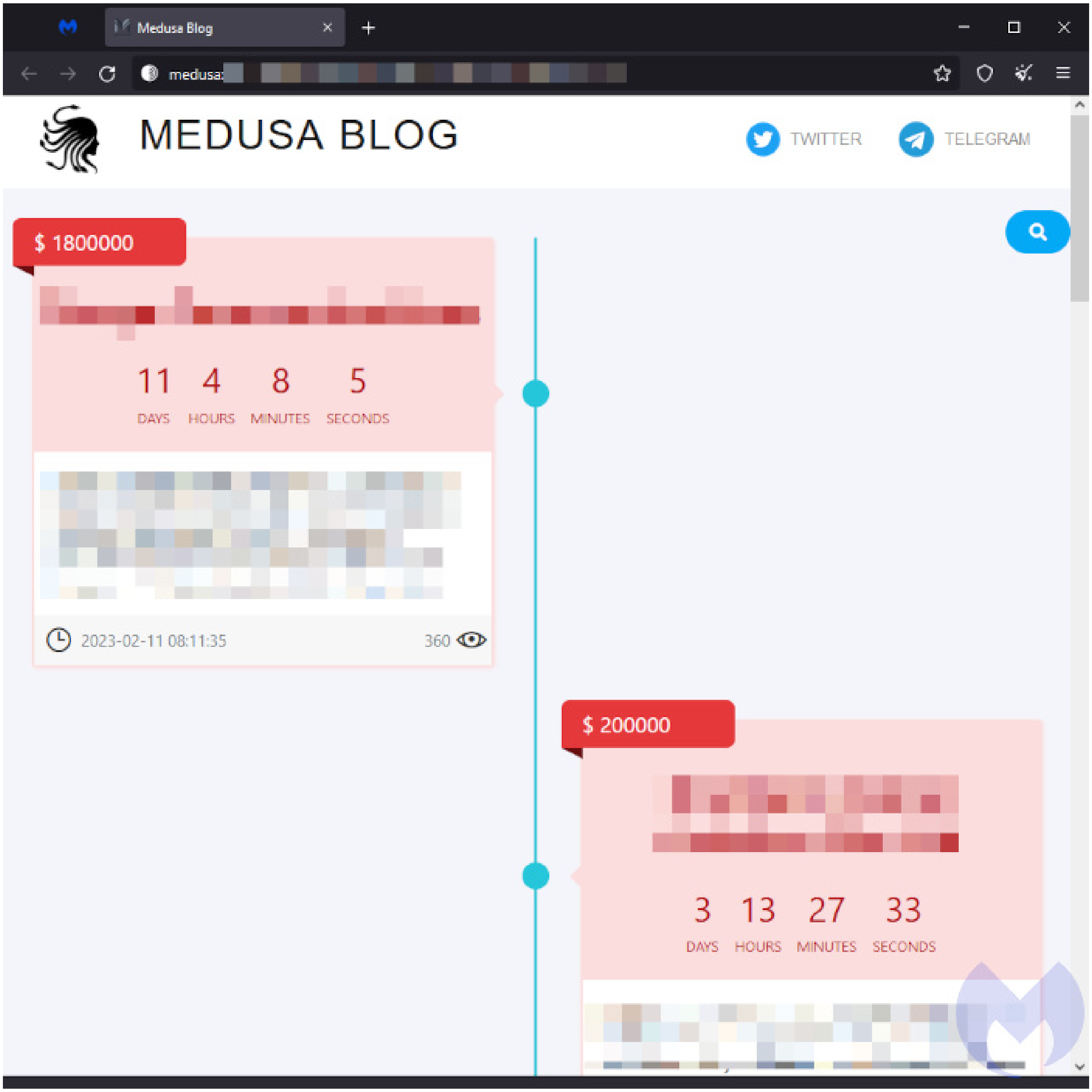
After LockBit, ALPHV (aka BlackCat) and Royal again topped the list of most known victims last month. But as it turns out, these two groups have more in common than just their high placements: Both are considered big dangers to healthcare organizations. The US Department of Health and Human Services (HHS) even released a detailed report on Royal and ALPHV in mid-January 2023 outlining the dual threat to the US health sector. Last month, however, Royal and ALPHV apparently only attacked one healthcare organization between them—ALPHV's attack on the Pennsylvania-based Lehigh Valley Health Network. Their combined 48 leaked victims last month were across a range of industries, mainly centered around manufacturing, logistics, and services. It just goes to show that just because ransomware is used to target one sector in one month that doesn't necessarily mean it won't be used against a different industry in another month.

Ever since we first reported on it in November 2022, witnessing the emergence of the Play ransomware gang over the months has been one of those "Aw, they grow up so fast (and evil)" type of situations. After their surge in December activity fell by about 76 percent in January, it made something of a comeback last month with 11 known victims, including the City of Oakland, where an attack shutdown many of the city's services. In fact, the situation was so bad in Oakland that the Interim City Administrator declared a state of emergency shortly afterwards.

New ransomware groups

Medusa

Not since we introduced Royal ransomware in November 2022 have we seen a new gang burst onto the scene with as much activity as Medusa did in February. The group published 20 victims on its leak site, making it the third most active ransomware last month. Among its victims are Tonga Communications Corporation (TCC), a state-owned telecommunications company, and oil and gas regulator company PetroChina Indonesia.



MEDUSA BLOG

$ 1800000

[redacted]

11	4	8	5
DAYS	HOURS	MINUTES	SECONDS

[redacted]

2023-02-11 08:11:35 360

$ 200000

[redacted]

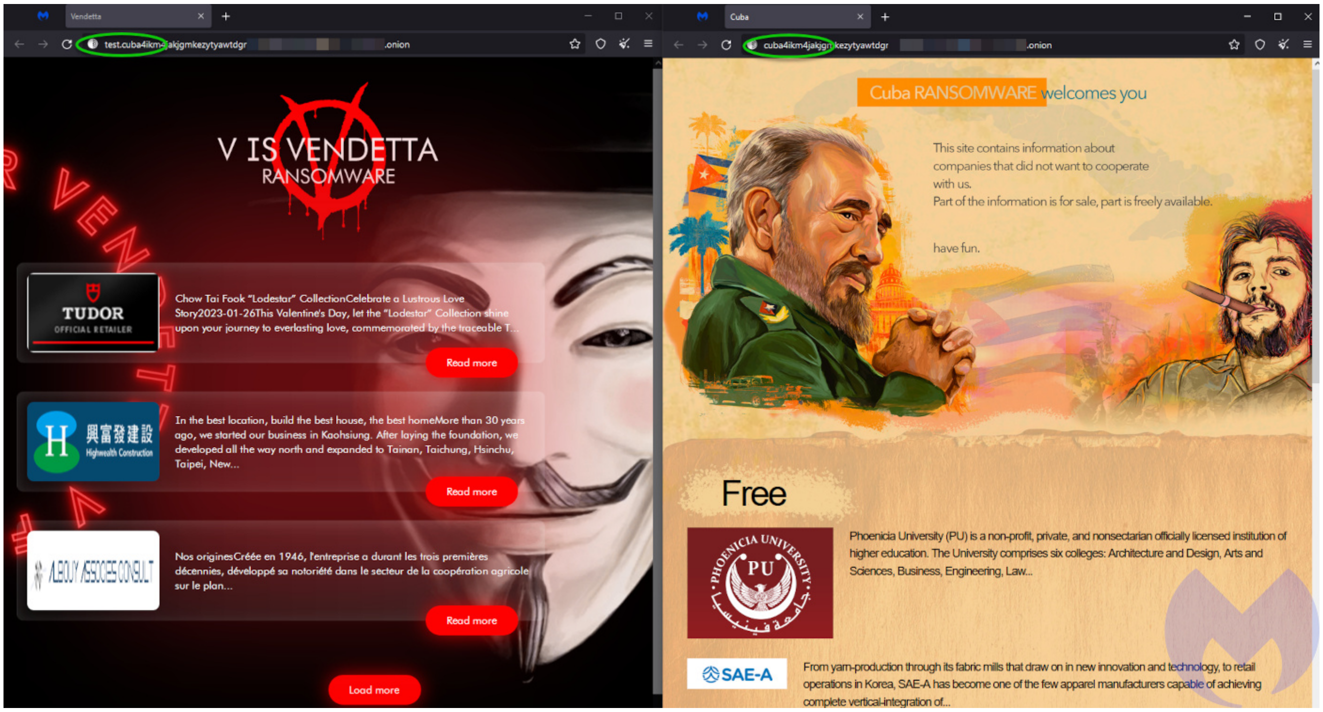
3	13	27	33
DAYS	HOURS	MINUTES	SECONDS

[redacted]

The Medusa leak site

V is Vendetta

V is Vendetta is a newcomer that published three victims in February on a site that follows the not-so-new practice of branding itself with imagery ripped from a particular mid-2000s dystopian action film. The site is noteworthy not only for its awful "teenager's bedroom" design but also for using a subdomain of the **Cuba** ransomware dark web site.



Chow Tai Fook "Lodestar" CollectionCelebrate a Lustrous Love Story2023-01-26This Valentine's Day, let the "Lodestar" Collection shine upon your journey to everlasting love, commemorated by the traceable T...

In the best location, build the best house, the best homeMore than 30 years ago, we started our business in Kaohsiung. After laying the foundation, we developed all the way north and expanded to Tainan, Taichung, Hsinchu, Taipei, New...

Nos originesCréée en 1946, l'entreprise a durant les trois premières décennies, développé sa notoriété dans le secteur de la coopération agricole sur le plan...

This site contains information about companies that did not want to cooperate with us.
Part of the information is for sale, part is freely available.

have fun.

Phoenicia University (PU) is a non-profit, private, and nonsectarian officially licensed institution of higher education. The University comprises six colleges: Architecture and Design, Arts and Sciences, Business, Engineering, Law...

From yarn-production through its fabric mills that draw on in new innovation and technology, to retail operations in Korea, SAE-A has become one of the few apparel manufacturers capable of achieving complete vertical-integration of...

The V is Vendetta leak site

DPRK's ransomware antics

In early February, CISA released an alert highlighting the continuous state-sponsored ransomware activities by the Democratic People's Republic of Korea (DPRK) against organizations in the US healthcare sector and other vital infrastructure sectors.

The agencies have reason to believe cryptocurrency ransom payments from such operations support DPRK's "national-level priorities and objectives." The report states:

> The authoring agencies assess that an unspecified amount of revenue from these cryptocurrency operations supports DPRK national-level priorities and objectives, including cyber operations targeting the United States and South Korea governments—specific targets include Department of Defense Information Networks and Defense Industrial Base member networks,

In the last few years, two new ransomware strains from DPRK have surfaced: Maui and H0lyGh0st.

US Marshal Service ransomware attack

It seems ransomware attackers are going after the big fish again.

At least, it's been a while since a federal agency like the US Marshals Service (USMS) was hit with ransomware. In late February 2023 a threat actor managed to infiltrate the agency and to get hold of sensitive information about staff and fugitives.

It's far from rare to see a ransomware attack on governments, to be sure. State, Local, Tribal, and Territorial (SLTT) governments were hammered by ransomware throughout 2022. Attacks on the federal government, however, remain few and far between.

If there's one thing this attack taught us, it's that no organization is safe from ransomware—but that's not all. It's also the most eye-catching attack on the fabric of the US since the Colonial Pipeline attack by the DarkSide ransomware gang. There is no word about who is responsible for the attack or whether or not there has been a ransom demand.

If this is the work of a regular ransomware gang rather than a political statement, it's a surprise that they're this bold (or frankly, stupid, for thinking the federal government would ever pay them). Attacking a federal government paints a huge target on their backs.

We know there have been times where affiliates of ransomware gangs go rogue and attack an organization that's off-limits according to the gangs' rules—but until more information is released, many details about the USMS breach remain speculative.

Our Ransomware Emergency Kit contains the information you need to defend against ransomware-as-a-service (RaaS) gangs.

GET THE RANSOMWARE EMERGENCY KIT

How to avoid ransomware

- **Block common forms of entry**. Create a plan for patching vulnerabilities in internet-facing systems quickly; disable or harden remote access like RDP and VPNs; use endpoint security software that can detect exploits and malware used to deliver ransomware.
- **Detect intrusions**. Make it harder for intruders to operate inside your organization by segmenting networks and assigning access rights prudently. Use EDR or MDR to detect unusual activity before an attack occurs.
- **Stop malicious encryption**. Deploy Endpoint Detection and Response software like Malwarebytes EDR that uses multiple different detection techniques to identify ransomware.
- **Create offsite, offline backups**. Keep backups offsite and offline, beyond the reach of attackers. Test them regularly to make sure you can restore essential business functions swiftly.
- **Write an incident response plan**. The period after a ransomware attack can be chaotic. Make a plan that outlines how you'll isolate an outbreak, communicate with stakeholders, and restore your systems.

COMMENTS

RELATED ARTICLES

ABOUT THE AUTHOR

Threat Intelligence Team