ZURICH
Resilience Solutions

Risk Topic

PYSA, seeking for unlawful admission to Schools and Colleges

On 16th March 2021, the FBI published a flash alert about the recent increase in PYSA ransomware targeting both US and UK educational institutions. In the UK, the National Cyber Security Centre also released a similar alert on 23rd March 2021 for the UKeducation sector without naming the PYSA variant.

Though first observed and reported in October 2019 when the group was targeting large corporates, PYSA got more public attention when CERT France issued analert in April 2020 that the variant was targeting Frenchlocal authorities.

PYSA is a new variant of ransomware to join the big names like Ryuk, Sobinokibi and Maze to target largefinance, government, education and healthcare organisations. It is a human-operated ransomware

Delivery

PYSA uses phishing or social engineering, or it is delivered by brute-forcing Remote Desktop Protocol credentials. Before detonating the ransomware payload, the APT group carries out network reconnaissance and installs tools to escalate privileges and spread laterally.

It is a new variant of Mespinoza ransomware which exfiltrates data from victims' systems before it encrypts files and appends the "PYSA" extension to the filename and uses it as leverage to demand ransom payments.

Some UK academic institutions even received phone calls directly from the APT Group, showing more aggression. The APT Group, in a thick Russian accent, advised that the institution had suffered a cyber-attack and their information was taken (no specifics around what details). The institutions were told to "act" to protect their information.

Neither call had any specifics as to timescales or actual ransom demands, only stating that PYSA was there to help and encouraging early attention.

This is a change of tactic for PYSA, having gone almost dormant from the end of last year. Previous intel does not record any previous calls or attempted calls.

The Risk

Like most new ransomware variants, PYSA uses double extortion tactics by exfiltration of sensitive personal data and then applying encryption to systems, causing business interruption as well as a potential of data breach of the exfiltrated sensitive information if released to the public upon non-payment of ransomware.

Along with significant time restore systems, these events also can become high profile and generate wide public and media interest.

Why the Education Sector?

The last 12 months have seen a significant increase in cyber-attacks on educational organisations across the world, where academic institutions have lost student coursework and financial records, as well as research data (hackers targeted the Oxford University laboratory engaged in COVID research in February 2021).

Universities are the home of cutting-edge research, which makes them an attractive target and more often this advanced work is not segregated in a separate network and thus vulnerable to any cyber-attacks on the wider university network.

Then there is always the huge repository of personal identifiable information on parents, students and alumni. These data sets can have a wide variety of data, from student loans and financial information to passport details and healthcare data.

Overall cyber maturity for academic bodies varies from basic to sophisticated, but the most difficult thing to control is the high volume of students and the use of their personal devices, with varying level of cyber controls, while accessing internal and external systems. When it comes to social engineering, tailgating, man- in-the middle attacks or planting USBs, it does not get easier than this environment. Every student and each device they use are a potential opportunity for a cyber-criminal.

The significant increase in remote learning due to COVID-19 has widened the attack surface for threat actors.

Mitigation

All the three alerts, FBI USA, NCSC UK and CERT France, include good recommendations to mitigate the risk of PYSA Ransomware attack.

But when considering controls to mitigate risks of PYSA or any other ransomware threats impacting both theconfidentiality and availability of information, organisations must take a structured approach

It is important to manage your digital footprint to reduce reconnaissance opportunities for cyber criminals. Find out what vulnerability information is available for the threat actor to exploit, like weaknesses in remote access configuration,

unwanted open ports, weak passwords and unpatched systems. Regularly scan and monitor these vulnerabilities and remediate them accordingly.

Apply controls to stop the delivery of malware by developing a cyber aware and phishing aware workforce, technical controls like email filters, Anti-Malware, Multi-factor authentication, IPS/IDS, etc.

If a threat actor manages to enter the organisation's environment, consider ways to stop the lateral escalation, privilege escalation and spreading of the infection. Some key controls to consider are network segmentation, up-to-date patching, strong passwords, privilege access management, and the use of multi-factor authentication for all admin accounts and access to highly sensitive information.

Finally, because there is always a chance that the threat actor will be successful in exploiting the weakness in the environment, two key considerations are:

Planning for cyber incident response, which is how you will respond when you suffer an attack. The plan must be accompanied by regular exercises for continuous improvement.

Disaster recovery planning with regular online and offline backup, testing the backup and recovery regularly for continuous improvement.

According to our Zurich UK's Strategic Cyber Risk Consultant, Arunava Banerjee, "Lockheed Martin's Cyber Kill Chain can be a very good strategy for an organisation to adopt for planning cyber risk mitigation controls by ensuring proportionate people, process and technical controls are in place at each level of the kill chain".

How can Zurich help?

Zurich Resilience Solutions helps clients to understand their level of maturity for handling ransomware with our Ransomware Readiness Service. The service identifies improvements that will enhance organisational cyber resilience against ransomware.

Our cyber consultants also help clients in developing their end-user cyber awareness strategy and cyber incident response maturity.

To provide a complete cyber mitigation advice, Zurich has partnered with cyber security companies who can provide specialist cyber and technical services for our clients at preferential rates.

Please get in touch with your account manager or other Zurich representatives to find out about our cyber risk management proposition and cyber partners.

References:

- https://www.ic3.gov/Media/News/2021/210316.pdf
- https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector
- https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-003/
- https://id-ransomware.blogspot.com/2019/10/mespinoza-ransomware.html
- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Risk Engineering UK
Risk Support Services
6th Floor, The Colmore Building
20 Colmore Circus, Queensway
Birmingham
B4 6AT

For further information about any of the topics mentioned in this document please speak to your local Zurich contact, or email Zurich Resilience Solutions at zrs.enquiries@uk.zurich.com or alternatively call this number +44 (0) 121 697 9131

For more information please visit: www.zurich.com/riskengineering

Zurich Management Services Limited, Registered in England and Wales no. 2741053,
Registered Office: The Zurich Centre, 3000 Parkway, Whiteley, Fareham, Hampshire PO15 7JZ