Quick Heal
Security Simplified

Quick Heal Technologies Ltd.

Regd. Office: Marvel Edge, Office No. 7010 C & D, 7th Floor,
Opposite Neco Garden Society, Viman Nagar, Pune 411014.
Tel: +91 20 66813232 | Email: cs@quickheal.co.in
CIN - L72200MH1995PLC091408

Ref. No.: QHTL/Sec/SE/2021-22/23 July 09, 2021

The Manager,
Corporate Services,
BSE Limited,
14th floor, P J Towers, Dalal Street,
Mumbai – 400 001
Ref: Security ID: QUICKHEAL
Security Code: 539678

The Manager,
Corporate Services,
National Stock Exchange of India Limited,
Exchange Plaza, Bandra Kurla Complex,
Bandra (E), Mumbai – 400 051
Symbol: QUICKHEAL
Series : EQ

Dear Sir/Madam,

Sub: Press Release pertaining to 'Suspected Pakistani APT group targeting Indian Critical Infrastructure PSUs'

Please find enclosed herewith a press release pertaining to 'Suspected Pakistani APT group targeting Indian Critical Infrastructure PSUs', for your records.

As permitted, this letter is being submitted under Sd/- mode due to work from home as per the Government advisory on Covid-19 and as a part of safety measure.

Please acknowledge receipt of this intimation.

Thanking you
For Quick Heal Technologies Limited

Sd/-

A. Srinivasa Rao
Company Secretary

Seqrite Report: Suspected Pakistani APT group targeting Indian Critical Infrastructure PSUs

- *Active since 2019, the Advanced Persisted Threat (APT) 'Operation SideCopy' appears to be cyber espionage campaign by Pakistan backed Transparent Tribe group against critical* Critical Infrastructure PSUs from telecom, power and finance sectors.
- *Seqrite is the first cybersecurity brand to identify and expose the 'Operation SideCopy' cyber-attack in 2020*

New Delhi, July 09, 2021: Seqrite, a specialist provider of enterprise cybersecurity products and solutions and the enterprise arm of Quick Heal Technologies Limited, has uncovered the second wave of APT campaign by operators of SideCopy Advanced Persistent Threat (APT). Researchers at Seqrite had exposed the operations of Operation SideCopy for the first time in 2020 and since last year and have come across a new wave of cyber espionage campaign by the attackers aimed at high profile targets from Critical Infrastructure PSUs from telecom, power and finance sectors.

Earlier during October 2020 Seqrite had come out with a report about Operation SideCopy APT targeting Indian Defence Units. This new finding has revealed that Operation SideCopy has expanded its target list to Critical Infrastructure. As part of the investigation, Seqrite researchers have discovered potentials links between Operation SideCopy and its operators to Pakistan.

According to the Seqrite report, threat actors were leveraging compromised websites, which resemble the websites that the targeted organizations would generally access. This shows that attackers did detailed reconnaissance before launching the attack campaign. Upon thorough analysis of the attack chain, the command-and-control (C2) server communication, and the available telemetry data, researchers at Seqrite could identify some compromised websites that are being used to host the attack scripts and act as C2 servers. Further analysis of data accessible from some C2 servers led researchers at Seqrite to an IP address that was commonly found across different C2 servers. In fact, this IP address turned out to be the first entry in many logs, which indicated that the corresponding system is likely being used for testing the attack before launch.

Further investigation of that IP, using data from whatismyipaddress.com, revealed that the provider of that IP address is Pakistan Telecommunication Company Limited. This revelation further strengthens the claim that Operation SideCopy which is operated by the Transparent Tribe group is originating in Pakistan. The report further revealed the list of targets that were identified through the analyzed C2s. These targets include Critical Infrastructure PSUs from telecom, power, and finance sectors. This is likely only a subset of targets since there are several other C2s being used in Operation SideCopy APT, which are probably targeting other entities.

Upon discovery, Seqrite researchers proactively alerted the Government authorities and are working with them to keep potential targets safe. Researchers suspect this attack to be a cyber-espionage campaign aimed at collecting sensitive information to gain a competitive advantage against India. The evidence gathered by Seqrite suggests a highly organized operation designed to evade most security mechanisms. As part of the campaign, attackers are sending out phishing emails with government-themed documents in an attempt to lure targets into opening the attachments.

According to Seqrite researchers, the malicious actors have enhanced the attack tools and methods, as compared to last year, to make detection difficult. The final payload can capture sensitive information including screenshots, keystrokes, & files from the affected system. In addition, it can also execute commands specified as part of instructions from C2 servers. This shows that this attack group is well funded and is actively improving its attack mechanisms to infiltrate the target entities. The group can potentially steal critical intel from the government agencies and their subsequent bodies. They can even use that information to make more lures and target other Government departments.

Anatomy of the attack

According to Seqrite's researchers, the initial intrusion chain begins with a spear-phishing email. The email content attempts to lure the user into extracting the attached zip archive. Upon extraction, the user would see a document file which is in fact an extension spoofed LNK file which is usually seen as shortcuts. If the user opens the document, the LNK payload gets launched and initiates the malicious activities in the background. To ensure the user is not suspicious, a decoy document is presented to him/her.

Once the LNK file is launched, it downloads the HTA payload from a compromised domain and executes it via mshta.exe. This HTA file is responsible for showing the decoy document to the user. In addition, it drops an executable of LimShell on disc and executes it. Most of the backdoors used in this campaign are variants of NJRat, however, in one specific case, we came across a new payload written in C# which installs an implant that helps the attacker examine the target and install other backdoors.

Seqrite threat intelligence team continually works towards the detection and prevention of attacks executed by multiple APT actors. It urges individuals and organizations to adhere to necessary cybersecurity protocols and use robust security solutions in addition to staying aware of the latest threats.

About Seqrite:

Seqrite is the cybersecurity security products & solutions brand of Quick Heal Technologies Limited that helps secure the digital transformation journey of enterprises and SMB firms. Launched in 2015, Seqrite solutions are defined by innovation and simplicity. A combination of intelligence, analysis of applications and state-of-the-art technology, Seqrite is designed to provide continuous and better protection for enterprise corporate customers.

Seqrite portfolio of solutions includes Endpoint Security, Enterprise Mobility Management (EMM), Unified Threat Management (UTM), Secure Web Gateway (SWG) and data protection technologies like Encryption and Data Loss Prevention (DLP). Besides, Seqrite Services provides comprehensive cybersecurity consulting services to Corporates, PSUs, Government and Law Enforcement Agencies. For more information, please visit: www.seqrite.com.

About Quick Heal Technologies Limited:

Quick Heal Technologies Limited is one of the leading providers of IT Security and Data Protection Solutions with a strong footprint in India and an evolving global presence. Incorporated in the year 1995, with a registered office in Pune, it is an all-round player in cybersecurity with presence in B2B, B2G and B2C segments across multiple product categories – endpoints, network, data and mobility.

With its state-of-the-art R&D centre and deep intelligence on the threat landscape, Quick Heal helps in simplifying security by delivering the best in class protection against advanced cyber-attacks. Its portfolio includes solutions under the widely recognized brand names 'Quick Heal' and 'Seqrite' across various operating systems and devices.

For more information, please visit: www.quickheal.co.in

For more information, please contact:
Akash Gosavi
M: +91 8007785096
E: akash.gosavi@quickheal.co.in