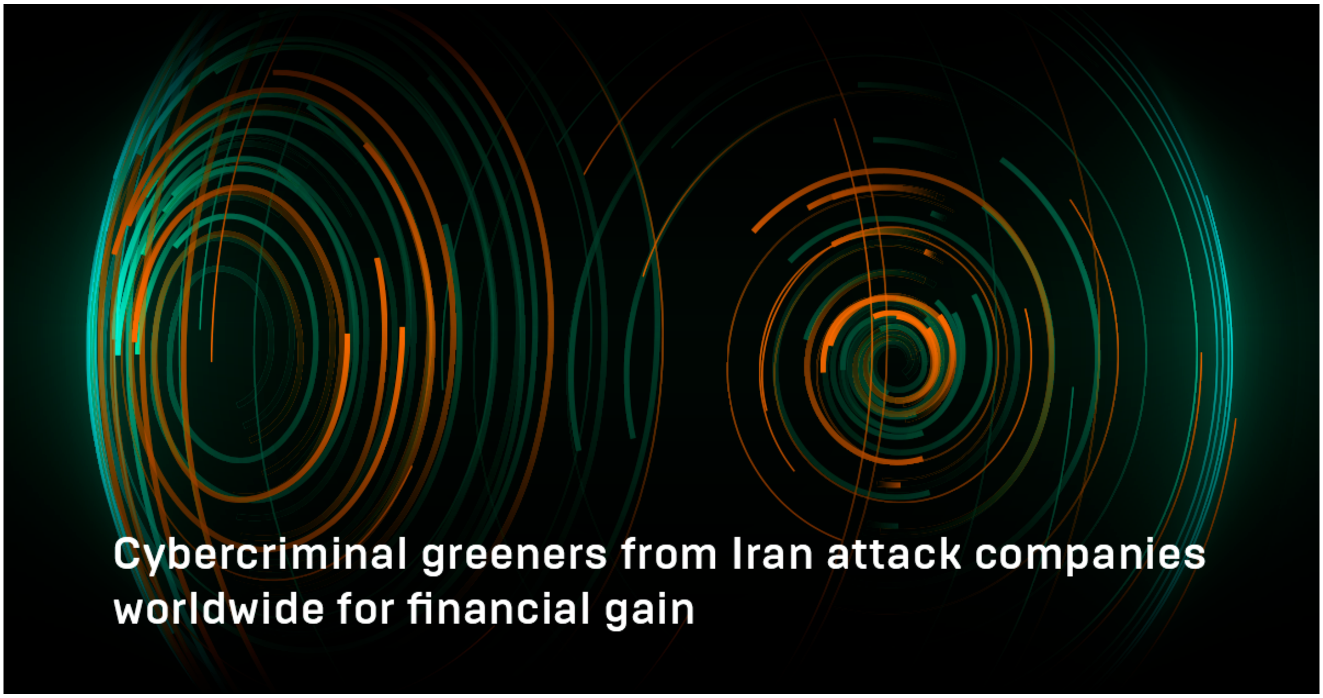
Cybercriminal greeners from Iran attack companies worldwide for financial gain

group-ib.com/media/iran-cybercriminals/



Group-IB, a global threat hunting and intelligence company headquartered in Singapore, has detected financially motivated attacks carried out by Iranian newbie threat actors in June. The attackers used Dharma ransomware and a mix of publicly available tools to target companies in Russia, Japan, China, and India. All the affected organizations had hosts with Internet-facing RDP and weak credentials. The hackers typically demanded a ransom between 1-5 BTC. The newly discovered hacker group suggests that Iran, which has been known as a cradle of state-sponsored APT groups for years, now also accommodates financially motivated cybercriminals.

Group-IB researchers have recently observed increased activities around Dharma ransomware distribution. Dharma, also known as Crysis, has been distributed under a ransomware-as-a-service (RaaS) model at least since 2016. Its source code popped up for sale in March 2020 making it available to a wider audience. During an incident response engagement for a company in Russia, Group-IB's DFIR team established that Persian-speaking newbie hackers were behind a new wave of Dharma distribution. Even though the exact number of victims is unknown, the discovered forensic artifacts allowed to establish the geography of their campaigns and the toolset, which is far behind the level of sophistication of big league Iranian APTs.

It was revealed that the operators scanned ranges of IPs for hosts with Internet-facing RDP and weak credentials in Russia, Japan, China, and India. To do so, they used a popular software called Masscan — the same technique was employed by Fxmsp, an infamous seller of access to corporate networks. Once vulnerable hosts were identified, the attackers deployed NLBrute to brute-force their way into the system and to check the validity of obtained credentials on other accessible hosts in the network. In some attacks, they attempted to elevate privileges using exploit for CVE-2017-0213.

Interestingly, the threat actors likely didn't have a clear plan on what to do with the compromised networks. Once they established the RDP connection, they decide on which tools to deploy to move laterally. For instance, to disable built-in antivirus software, the attackers used Defender Control and Your Uninstaller. The latter was downloaded from Iranian software sharing website — the Google search query in Persian language “دانلود نرم افزار youre unistaller” was discovered in the Chrome artifacts. Other tools were downloaded by the attackers from Persian-language Telegram channels when they were already present in the network.

To scan for accessible hosts in the compromised network, threat actor used Advanced Port Scanner — another publicly available tool. After the network reconnaissance activities were completed, the adversary used collected information to move laterally though the network using the RDP protocol. The end goal of the attackers was to drop and execute a variant of Dharma ransomware: the adversary connected to the targeted hosts, dropped Dharma executable, and executed it manually. On average, the ransom demand was between 1-5 BTC.

The fact Dharma source code has been made widely available led to the increase in the number of operators deploying it. It's surprising that Dharma landed in the hands of Iranian script kiddies who used it for financial gain, as Iran has traditionally been a land of state-sponsored attackers engaged in espionage and sabotage. Despite that these cybercriminals use quite common tactics, techniques and procedures they have been quite effective. Therefore, we believe it's important to provide some recommendations on how to protect against them and give a complete outline of the MITRE ATT&CK mapping.

Oleg Skulkin

Senior Digital Forensics Specialist

The pandemics exposed a great number of vulnerable hosts with many employees working from homes and the vector became increasingly popular among cybercriminals. Therefore, the default RDP port 3389 should be edited by changing it to any other. As the attackers usually need several attempts to brute force passwords and gain access to the RDP, it is important to enable account lockout policies by limiting the number of failed login attempts per user. Threat intelligence solutions enable organizations to mitigate risks and further damage by quickly identifying stolen data and tracking down the source of the breach, while specialized threat detection systems allow to discover unwanted intrusions, traffic anomalies within the corporate network, and attempts to gain unauthorized access to any data.