CYLANCE

OPERATION CLEAVER
Frequently Asked Questions

What Enterprises And Consumers Need To Know

Q: Why did Cylance® release this information?
Due to the choice of critical infrastructure victims, Iran's quickly improving skillset and potential global impact, we are compelled to write this report, exposing our intelligence on Cleaver with the hopes the information we share can reveal the techniques and tools of this group, drawing global attention and preventing attacks which could endanger human lives.

Q: What were the goals of the attackers?
The attackers first sought to gather intelligence on the facilities and employees at the hacked organizations but later proved to have completely compromised systems and networks. The methods and tools used to sustain persistence and the economic and governmental sensitivity pre-supposes true harm beyond just intellectual property or financial gain.

Q: What were the attackers pursuing?
The most troubling was compromise of transportation networks and systems such as airlines and airports in South Korea, Saudi Arabia and Pakistan. We also uncovered swaths of sensitive and specific identifiable information: employee data such as schedule details, VPN credentials, identification photos, housing details, timecards, passports, and social security cards. We also found information related to facility security, including video network diagrams, blueprints, and security codes.

Q: What tactics did the attackers use?
Iran's skills are advancing beyond their past history of website defacement, distributed denial of service, and similar basic techniques. The attackers used a variety of approaches, both publicly available and proprietary to the group. They primarily used SQL injection, spear phishing and water holing. They also used a proprietary botnet infrastructure called "tiny Zbot".

Q: Who were the attackers?
Our investigation is ongoing but we have observed a primary team named "Tarh Andishan" which has compromised more than 50 victims in just the past two years.

Q: What countries and organizations were affected by these attacks?
The victim organizations are based all over the world, with emphasis on organizations and facilities in Pakistan, South Korea, UAE, Qatar, Kuwait and various European countries. The United States was also a target, although other countries' infrastructure was attacked more aggressively. These targets include airlines, airports, oil & gas, manufacturing, technology government and universities.

Q: Were these groups associated with any terrorist organizations?
Our work mainly focused on discovering compromised networks and the data that was stolen from the victims. We are not in a position to make those kinds of connections.

Q: When did the attacks first occur?
The first evidence we could find of this group actively hacking was from June 2012, however, we believe they may have started as early as 2010. We believe the attacks are ongoing.

Q: What kind of targets did the attackers go after?
Multiple Iranian hacker teams successfully attacked and compromised targets in a variety of industries (16) with a focus on transportation, airports and airlines, energy, oil and gas, telecommunications, education and government.

Q: Why were the attackers going after these targets?
We are not in a position to comment on all of their intentions, but from what we have seen, they appear to be hacking with the intent to cause harm to global critical infrastructure. They do this by cyber disruption and by coordinating the release of sensitive information to outside groups.

Q: Were these attacks coming from the Iranian government?
While we are not privy to the information that would be required to make this kind of connection, we have observed a hacker team named Tarh Andishan, based out of Tehran, which has attacked and compromised more than 50 victims in the past two years.

Q: Do think that Iran is now a global top tier cyberthreat?
The type of attacks we've observed show sophistication in approach and organization. Additionally, the geo-political impact of the targets infers Iran is a source of serious cyberthreat participants.

Q: In your report, you reveal that organizations in Korea were a major target. Do you believe the hackers were working with North Korea to carry out these attacks?
As cybersecurity experts, we avoid speculating on specific political matters. However, we can say generally we have found nations will often barter cybersecurity services and use these abilities to increase their technical clout and political power.

Q: What does this mean for businesses and organizations that might be potential targets?
We are facing an inflection point in technology, and for far too long the industry approach to cybersecurity has been to play detect and respond to hackers. We really need a paradigm shift in the industry, and that's what we're doing at Cylance, as evidenced by this discovery. Through math and machine learning, our product was able to uncover the previously undiscovered malware that was being used in these attacks. We can never know exactly what the next attack will look like, or where it will come from, but we can build a smarter security product that intelligently analyzes potential threats and prevents them from ever executing.

Q: Did you notify the companies that were affected by these attacks?
Cylance is committed to responsible disclosure. We have notified all known victims discovered during our investigation, prior to the publishing of this report.

Q: Are you working with law enforcement on this issue?
We always work closely with law enforcement when the situation requires it. These findings have prompted us to work closely with law enforcement for validation and due process.

Q: How do I know if I'm affected?

If your organization fits into any of the following categories; transportation, airports and airlines, energy, oil and gas, telecommunications, education and government, you are at a higher risk of being a target. However, if you have CylancePROTECT® installed in your network and on your endpoints, you are better protected. If you have any concerns, we will gladly work with you to provide a compromise assessment.

About Cylance:

Cylance is the first company to apply artificial intelligence, algorithmic science and machine learning to cybersecurity and improve the way companies, governments and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist. By coupling sophisticated machine learning and artificial intelligence with a unique understanding of a hacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats. For more information, visit cylance.com

+1 (877) 973-3336
sales@cylance.com
www.cylance.com
18201 Von Karman, Ste. 700, Irvine, CA 92612

CYLANCE