ERT Threat Alert

Revenge of the Students: Cyber-Attacks Target Schools

May-19-2016

Abstract

The cyber-attack in Japan last week that took down 444 school networks simultaneously is the latest example of a worldwide trend: student-launched cyber assaults targeting educational institutions via online hacking services and tools.

Radware's 2015-2016 Global Application & Network Security Report predicted an increase in cyber-attacks against educational institutes. This corresponds to the growing variety of powerful attack tools available to novice attackers via the Darknet.

Motivations

In most cases, it's either a student looking to delay a test, manipulate the registration process or a personal attack by a student or staff member in aggression towards the school.

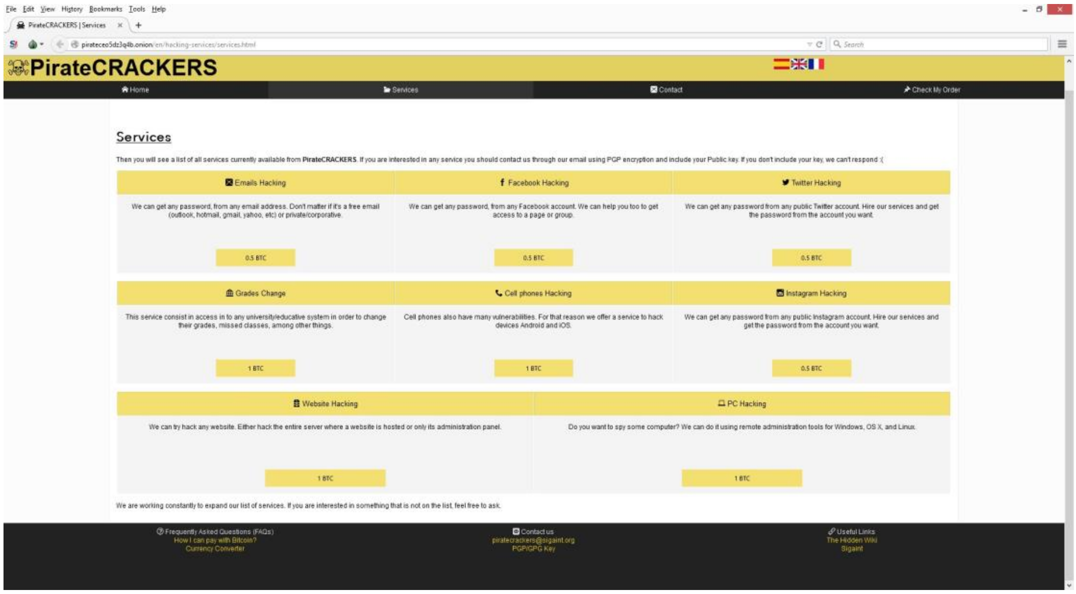
Common Attack Methods

- SQL injections
- UDP reflective attacks such as:
  - DNS flood
  - NTP flood
  - SNMP flood

Attackers will target online educational platforms like Blackboard and Moodle, student portals, admission processing site, mail servers, or databases contacting personal or sensitive information. These attacks jeopardize an institution's reputation and disrupt the students' learning process, affecting the institution's business operations and services.

Reasons for Concern

One reason for concern is the growth of school hacking services found on the Darknet. Vendors will offer services such as grade changes and denial of service attacks for hire. This makes it increasingly easy for non-hackers to carry out an attack or cause damage to a school's resources. In addition to these services, a potential attacker can rent botnets or stresser services for Bitcoin (see Figure 1 below).


File Edit View History Bookmarks Tools Help
PirateCRACKERS | Services
pirateceo5dz3q4b.onion/en/hacking-services/services.html
Search
PirateCRACKERS
Home
Services
Contact
Check My Order

Services

Then you will see a list of all services currently available from **PirateCRACKERS**. If you are interested in any service you should contact us through our email using PGP encryption and include your Public key. If you don't include your key, we can't respond :(

Emails Hacking

We can get any password, from any email address. Don't matter if it's a free email (outlook, hotmail, gmail, yahoo, etc) or private/corporative.

0.5 BTC

Facebook Hacking

We can get any password, from any Facebook account. We can help you too to get access to a page or group.

0.5 BTC

Twitter Hacking

We can get any password from any public Twitter account. Hire our services and get the password from the account you want.

0.5 BTC

Grades Change

This service consist in access in to any university/educative system in order to change their grades, missed classes, among other things.

1 BTC

Cell phones Hacking

Cell phones also have many vulnerabilities. For that reason we offer a service to hack devices Android and iOS.

1 BTC

Instagram Hacking

We can get any password from any public Instagram account. Hire our services and get the password from the account you want.

0.5 BTC

Website Hacking

We can try hack any website. Either hack the entire server where a website is hosted or only its administration panel.

1 BTC

PC Hacking

Do you want to spy some computer? We can do it using remote administration tools for Windows, OS X, and Linux.

1 BTC

We are working constantly to expand our list of services. If you are interested in something that is not on the list, feel free to ask.

Frequently Asked Questions (FAQs)
How I can pay with Bitcoin?
Currency Converter
Contact us
piratecrackers@sigaint.org
PGP/GPG Key
Useful Links
The Hidden Wiki
Sigaint

Figure 1: PirateCRACKERS offering grade changing services

Attack Vectors

1. **UDP Flood** - A UDP flood is a network flood and still one of the most common floods today. The attacker sends UDP packets, typically large ones, to a single destination or to random ports. In most cases the attackers spoof the SRC IP which is easy to do since the UDP protocol is "connectionless" and does not have any type of handshake mechanism or session. The main intention of a UDP flood is to saturate the Internet pipe. Another impact of this attack is on the network and security elements on the way to the target server, and most typically the firewalls. Firewalls open a state for each UDP packet and will be quickly overwhelmed by the UDP flood.

2. **Reflection Attacks** – Reflective denial-of-service attacks makes use of a potentially legitimate third-party component to send the attack traffic to a victim, ultimately hiding the attackers' own identity. The attackers send UDP packets to the reflector servers with a source IP address set to their victim's IP, therefore indirectly overwhelming the victim with the response packets. The reflector servers used for this purpose could be ordinary servers with no indication/trace that they have been compromised, which makes this kind of attack particularly difficult to mitigate. A common example for this type of attack is DNS, NTP, and SNMP reflection.

3. **SQL Injection** - Exploiting poor coding of web application where the inputs are not sanitized therefore exposing application vulnerabilities. SQL injection is the most common type of injection attack which also count LDAP or XML injections. It is by far the number one vulnerability listed in OWASP Top 10. The idea behind a SQL injection is to modify an application SQL (database language) query in order to access or modify unauthorized data or to run malicious programs. Most web applications rely on databases where the application data is stored and being accessed by SQL queries and modifications of these queries could mean taking control of the application.

Recently Targeted Schools

- **Japan**[i] – A 16-year-old student in Japan downloaded an attack tool to his desktop and carried out an attack on the Osaka Board of Education server, resulting in 444 elementary, junior highs, and high school websites being knocked offline. He was monitoring the attack from his cellphone and expressed that he wanted to join Anonymous, the worldwide hacktivist group. This student ultimately launched this attack due to his frustration with his school teachers.

- **Australia**[ii] – A 15-year-old in Australia is facing 10 years in jail for launching one of the largest DDoS attacks in the country's history. The attack was so large that around 10,000 customers for the local ISP NuSkope were also affected. This attack was directed at a number of targets including Reynella East College. The attacker said that he launched the assault as a test.

- **India**[iii] – A college in India was hacked and defaced by a group named Pak Cyber Attacker. The attack was launched against both the official website of Utkal University and the e-admissions page. At the time of this report, the e-admissions page was not accessible.

- **Canada**[iv] – A Vancouver high school suffered network service degradation following a student successfully compromising his/her teacher's email account and began spamming out emails in bulks to a list of over 50,000 email addresses. This action of spamming slowed down the school's network operation. The student was expelled.

- **England** – Janet[v], a research and educational network in England, has been the victim of several denial-of-service attacks over the last year. Janet connects the networks of 19 different regional universities. The sophisticated attacked rippled through these networks, resulting in degradation to network services and performance.

- **United States** – Rutgers[vi], Arizona State University[vii] and University of Georgia[viii] have all experienced denial-of-service attacks over the last year. These attacks have caused a number of issues resulting in delays during registration and final exams. Often times these attacks are so large that they completely saturate the network, preventing students from being able to connect to the network.

Organizations Under Threat Should Consider

Protection from UDP Floods, reflection attacks and other DDoS techniques:

- A hybrid solution combining on-premise detection and mitigation with cloud-based protection for volumetric attacks. It facilitates quick detection, immediate mitigation and internet pipe saturation.
- Solution must distinguish between legitimate and attack traffic, blocking it while protecting the SLA.
- An integrated, synchronized solution that can protect from multi-vector attacks combining DDoS with web-based exploits such as website scraping, Brute Force and HTTP floods.
- A cyber-security emergency response plan that includes a dedicated emergency team of experts.

Protection from SQL injections and web application vulnerabilities:

- IP-agnostic device fingerprinting – the ability to detect attacks beyond source-IP by developing a device fingerprint that enables precise activity tracking over time.
- Automatic and real time generation of policies to protect from zero-day, unknown attacks.
- Shortest time from deployment to a full coverage of OWASP Top-10.
- Radware's hybrid attack mitigation solution provides a set of patented and integrated technologies designed to detect, mitigate and report the most advanced threats. Dedicated hardware and cloud solutions protect against attacks in real time and help ensure service availability.

Under Attack and in Need of Expert Emergency Assistance?

Radware offers a full range of solutions to help networks properly mitigate attacks similar to these. Our attack mitigation solutions provide a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced DDoS attacks and cyber threats. With dedicated hardware, fully managed services and cloud solutions that protect against attacks, Radware can help ensure service availability. To understand how Radware's attack mitigation solutions can better protect your network contact us today.

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

[i] http://news.softpedia.com/news/japanese-kid-wannabe-anonymous-member-shuts-down-444-schools-with-ddos-attacks-504151.shtml

[ii] http://www.adelaidenow.com.au/news/south-australia/teen-charged-over-cyber-attacks-at-a-school-internet-service-provider-and-government-agency/news-story/57e0112794f8aee5daea49e4174b9ea1

[iii] http://www.newindianexpress.com/states/odisha/PG-admissions-Utkal-University-shifts-to-offline-mode-after-hacking-attempts/2016/05/10/article3425832.ece

[iv] http://www.fox19.com/story/31800780/vancouver-student-expelled-for-hacking-high-school-email-system

[v] http://www.theregister.co.uk/2016/04/18/janet_clobbered_with_ddos_attacks_again
[vi] http://news.softpedia.com/news/rutgers-university-suffers-sixth-ddos-attack-this-year-498229.shtml
[vii] http://college.usatoday.com/2015/05/04/arizona-state-rutgers-battle-web-blockages-a-week-before-finals/
[viii] http://www.ajc.com/news/news/local-education/university-of-georgia-hit-by-cyberattack/nqtN9/