Yui Kee Computing Ltd.

Newsletter

March 2012

Contents

University of Michigan hacks Washington DC Election

<web-link for this article>

In 2010, Professor Alex Halderman from the University of Michigan took up an open invitation from the Washington DC election board to hack their new e-voting system for absentee ballots. Halderman and his team quickly found multiple vulnerabilities that they used to stuff the ballot and modify the system, including causing the site to play the University of Michigan football fight song after user logout.

The successful attack went undiscovered for two days, when another tester reported that the system was secure, but that the annoying music on the sign-off screen should be removed.

Halderman has now published a full account. The details include initial access by a shell injection vulnerability and use of username "admin", password "admin" for a terminal server account. They also used the voting system monitoring cameras to check when staff had gone home so that their server activity would go unnoticed. They added fictional characters to the candidate list, and elected Futurama character Bender as head of a school board. They could change all past and future ballots on the system.

The attack highlights the technical difficulties in developing secure electronic voting systems. Another concern with e-voting is that permitting voters the convenience of voting anywhere greatly reduces the protection against vote buying and voter intimidation that a secure voting booth provides.

More Information

Attacking the Washington, D.C. Internet Voting System
Election hacked, drunken robot elected to school board

Fraudster Couldn't Fool Sensitive Octopus

<web-link for this article>

In the first case of its kind, a technician and his family have been arrested for allegedly defrauding MTR Corp and Octopus Cards of HK$430,000. The Octopus card is a contactless smartcard commonly used for payments on public transport and retail outlets in Hong Kong. The technician arrested formerly worked for a contractor responsible for maintaining the Octopus card readers. It is alleged that he stole card reader parts from a storeroom, later assembled a working add-value machine that could accept banknotes at his home and family members assisted in using the cards to purchase items that could be resold.

The fraud was detected from company records that revealed value being added to cards by a machine that was not on the Octopus network. Police then investigated people employed by MTR Corp or its contractors who had access to add value machines. Superintendent Glenn O'Neill said, "Creating an add-value machine requires insider technology or high-level technical expertise."

Yui Kee's Chief Consultant, Allan Dyer commented, "This shows the value of defence in depth and audits. The technical features of the card and the payment system make changing the value on the card without an authorised reader almost impossible, but here an authorised reader was stolen, bit by bit. The reconciliation of records revealed the crime, and the access restrictions on equipment limited the personnel that the Police needed to investigate."

More Information

Octopus whiz-kid held over $430,000 machine scam

Cybercriminals Target Hong Kong Gold Exchange

<web-link for this article>

Police are investigating cyber attacks on the Chinese Gold and Silver Society, which operates Hong Kong's biggest commodities trading floor, and their traders.

Exchange chief executive Haywood Cheung Tak-hay said that eight members suffered serious attacks over the last two weeks. Before then, there were only minor attacks on one or two members. The incidents were reported to the Police on 16 March and included posting false rumours about exchange members being investigated by the Independent Commission Against Corruption (ICAC) and denial of service attachs against online trading systems. The criminals followed up the attacks with extortion demands for HK$100,000. Cheung said that the attacks probably originated from China, Australia and New Zealand.

It is reported that the exchange is installing anti-spam software as a prevention method. The Police emphasised its cooperative efforts with spcialists to counter the rise of similar crimes, with a spokesperson saying, "Given the increase in such cases, the police held many discussions with industry players over the past year. With the co-operation of IT specialists, the police enabled e-commerce entities to increase their ability to counter cyberattacks."

In an Editorial on the attacks, local English-language newspaper the South China Morning Post expressed its opinion of the attackers:

> But when it comes to internet security, nothing is more dangerous than complacency. Perhaps, for that reason, while hackers are criminals, they should also be thanked. If it were not for their dogged determination to break through security barriers, whether for the thrill or the challenge, to vandalise or to steal data, they at least highlight vulnerabilities that have been overlooked. It is for this reason that some firms hire hackers to seek out failings so that websites can be as watertight as possible.

Yui Kee's chief consultant hit out at the newspaper's attitude, "I think it is deplorable that a respected newspaper is advising hiring known criminals for their criminal knowledge. How is this different to paying the extortion? There are people who specialise in breaking into systems

that have never committed a crime, sometimes they are called Penetration Testers, or White Hat Hackers, or Ethical Hackers, but they need a broader range of skills than a criminal hacker. A criminal hacker merely needs to find a single hole in the defences to make a successful attack, and some know less than that, merely being 'script kiddies' that can run tools created by more skilled people. A diligent penetration tester will try to find every possible hole in the target's defences, identifying them so that they can be fixed. If you are burgled, do you buy new locks from your burglar?"

Note: It is not possible to provide a permanent link to the South Morning China Post articles referred to here because the paper's website uses temporary links and has a paywall. The news item was headlined, "Hackers bombard gold exchange" and the editorial was, "Complacency puts websites in danger", both published on 23 March 2012.

More Information

South China Morning Post
Police probe hacking of trading system
Cops probe web blackmail bid

March Hong Kong Honeypot Report

<web-link for this article>

This is the third monthly report from West Coast Labs's honeypot in Hong Kong, providing some indication of the type and level of malware threat in Hong Kong, but it is only based on a single honeypot, so the conclusions should be treated with caution. The number of attacks has dropped this month, and Canada tops the list of the commonest source for the first time.

Average Time To Infect: 15 hours 49 minutes

The average time to infect is an indication of how long it would be before a vulnerable computer connected to the internet in Hong Kong became infected. Two hours longer than previously.

Summary

- Total number of attacks : 44
- 25 are brand new to this honeypot.
- 10 of these files have not been seen in other honeypots

Source of Attacks

The following breaks down where these attacks have come from by use of IP geolocation.

Number of attacks	Source
8	Canada
7	United States
7	Japan
4	Saint Lucia
4	Thailand
2	Germany
1	Finland
1	Taiwan
1	Ukraine

1	Macedonia
1	Malaysia
1	Romania
1	Korea, Republic of
1	Vietnam
1	India
1	Hungary
1	Egypt
1	China

Canada, the United States and Japan are the top sources this month.

Malware List

Checksum (md5)	This month	Previous count	Detection
524412854e3e07f03daa94f52732fd5a	1	0 ***NEW	Y (W32/Virut.7116, Net-Worm.Win32.Kolab.epr , ,)
61750fceda6d2d955ffe39406323a900	1	0 ***NEW	Y (W32/Virut.7205, Backdoor.Win32.Rbot.adqd , ,)
5cfc941ac811a6cb7eb689b10b623965	1	0 ***NEW	Y (W32/EmailWorm.AMX, Net-Worm.Win32.Allaple.b , ,)
27e0cb71d5229bf0290590dc9eef70ba	1	0 ***NEW	Y (w32/allaple.h , trojan.win32.genome.rioo Net-Worm.Win32.Allaple.e , ,)
01217b54b0c96a9a7a21b7525b303f19	1	0 ***NEW	Y (W32/Allaple.C, Net-Worm.Win32.Allaple.b , ,)
d3e06bd6807fed271a0999eaf15b191e	1	0 ***NEW	Y (W32/GenBl.D3E06BD6!Olympus, Trojan.Win32.VBKrypt.kbuc Net-Worm.Win32.Kido.ih , ,)
a53d42b903c73c6f3a344839544cc86f	1	0 ***NEW	Y (W32/Allaple.A.gen!Eldorado, Net-Worm.Win32.Allaple.e , ,)
a0f7bc4600b926cc466c3f1328482088	1	0 ***NEW	Y (W32/Virut.7116, Virus.Win32.Virut.av Net-Worm.Win32.Allaple.e , ,)
624223c0add992ad25ace18a0e04a948	1	0 ***NEW	Y (W32/RAHack.A.gen!Eldorado, Net-Worm.Win32.Allaple.b , ,)
208ad942d625713918bc9e1907d843af	1	0 ***NEW	Y (, Trojan-Dropper.Win32.Injector.cybi , ,)
4fef2f0068be9a49fc23b67b4e0c0b09	1	0 ***NEW	Y (W32/EmailWorm.HQK, Net-Worm.Win32.Allaple.e , ,)
ceaa9adf344f3bf47fff1d1cf19a58a1	1	0 ***NEW	Y (W32/Virut.7116, Net-Worm.Win32.Allaple.e , ,)
820dc20fab3125fefd3ebff3ab4e0f0f	5	0 ***NEW	Y (W32/GenBl.820DC20F!Olympus, Trojan.Win32.Jorik.Poebot.ce , ,)
59f45bee28c9e31145ef7a2ef7a66ef7	8	0 ***NEW	N (, , ,)
a78b07e6875c8a0702ce855bf41d0abb	4	0 ***NEW	N (, , ,)
e3bb292eff0a5bfbf768f42dcbea845d	1	0 ***NEW	Y (W32/WormX.TV W32/Allaple.H , trojan.win32.genome.rioo Net-Worm.Win32.Allaple.e , ,)
bf79e90feed96f50c0ba5d7f212757e9	1	0 ***NEW	Y (w32/agent.ix.gen!eldorado , Trojan-Spy.Win32.Agent.bmxb trojan-spy.win32.agent.bmxb , ,)
06eaaf68e98a39b2085d5c15f40bf298	1	0 ***NEW	Y (W32/RAHack.A.gen!Eldorado, Net-Worm.Win32.Allaple.b , ,)
c896319a2f711580ce9fcb1160eadcef	1	0 ***NEW	Y (W32/Allaple.A.gen!Eldorado, Net-Worm.Win32.Allaple.e , ,)
48a23388878a981bf058b26f659ddb05	1	0 ***NEW	N (, , ,)
f11d86b86efb1d523a07ec8bcb94a61e	1	0 ***NEW	N (, , ,)
9e299dd7ecc7e286d33f962275a1053b	1	0 ***NEW	Y (W32/Allaple.A.gen!Eldorado, Net-Worm.Win32.Allaple.e , ,)
9be443d09b25157fcfbccb953f4a2cd4	4	4	N (, , ,)
979ed4871eb7ca2dad69c48cd924f4d5	1	1	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)

6280aa5062ee0e5a94b26fa85ae76d5d	1	0 ***NEW	Y (W32/Sdbot.AEFV , Backdoor.Win32.Rbot.adqd , ,)
07f43e524ea20e1a5677e8ae7434ebdb	1	0 ***NEW	Y (W32/Virut.7116, , ,)
12fb7332920a7797c2d02df29b57c640	1	0 ***NEW	Y (W32/Trojan2.KEXN , Trojan-Spy.Win32.Agent.bmxb, ,)

Note

The parameter 'Detection' here relates to whether one or more scanners was able to associate a name with this checksum.

More Information

- January Hong Kong Honeypot Report
- West Coast Labs

YUI KEE 銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/