SK Hack by an Advanced Persistent Threat

Command Five Pty Ltd

September 2011

Abstract

This document summarises the July 2011 intrusion into SK Communications which culminated in the theft of the personal information of up to 35 million people. It describes the use of a trojaned software update to gain access to the target network, in effect turning a security practice into a vulnerability. It also describes the use of a legitimate company to host tools used in the intrusion. Links between this intrusion and other malicious activity are identified and valuable insights are provided for network defenders. Technical details of malicious software and infrastructure are also provided.

Warning

This paper discusses malicious activity and identifies Internet Protocol (IP) addresses, domain names, and websites that may contain malicious content. For safety reasons these locations should not be accessed, scanned, probed, or otherwise interacted with unless their trustworthiness can be verified.

SK Hack

On 28 July 2011 SK Communications announced it had been the subject of a hack which resulted in the theft of the personal details of up to 35 million of its users. The compromised details were those of CyWorld and Nate users, as stored in SK Communications' user databases. CyWorld[1] is South Korea's largest social networking site and Nate is a popular South Korean web portal. Both services are owned by SK Communications. (Sung-jin, 2011)

The sophistication of the attack along with the period of time over which it was planned, and conducted, indicate that this attack was likely to have been undertaken by an Advanced Persistent Threat[2].

Between 18 and 25 July 2011 the attackers[3] infected over 60 SK Communications computers and used them to gain access to the user databases. The attackers infected these computers by first compromising a server, belonging to a South Korean software company, used to deliver software updates to customers (including SK Communications). The attackers modified the server so that the SK Communications computers would receive a trojaned[4] update file when they conducted their routine checks for software updates. (Moon-young, 2011) (ESTsoft, 2011)

[1] CyWorld has also expanded to China, Japan, the United States, Taiwan, Vietnam and Europe. (SK Communications)

[2] For a definition of the term 'Advanced Persistent Threat' refer to the Command Five paper 'Advanced Persistent Threats: A Decade in Review' (Command Five Pty Ltd, 2011).

[3] The term 'attackers' is used in this paper to describe both the hackers and anyone to whom they were reporting.

[4] A trojan is a document or program which appears harmless but performs malicious activity when opened or run.

Such routine updates (commonly known as 'patches') are a good security practice as they often include fixes for security weaknesses identified in the software. Without software updates the SK Communications computers would have been vulnerable to several other attacks including a significant one which was made public in June 2011[5]. The security of software updates is usually trusted implicitly and the exploitation of this trust relationship could go undetected by many targets, as it did for some time by SK Communications.

Between 18 and 25 July the attackers conducted command and control and monitoring activities on the infected computers. This involved the upload of tools, conveniently stored on the website of a Taiwanese publishing company the attackers had earlier hacked. Then on 26 July 2011, the attackers, having done the necessary groundwork, proceeded to hack the Nate and CyWorld user databases[6]. (Birdman, 2011) (Moon-young, 2011)

Using 'waypoints'[7] to obfuscate the source of their activities, the attackers successfully stole the personal details of up to 35 million SK Communications customers from the user databases. These personal details included names, phone numbers, home and email addresses, birth dates, gender details, user identifiers, passwords and, due to South Korea's Real Name System[8] which was in place at the time, also resident registration numbers. The passwords and resident registration numbers were reportedly encrypted but the other details were not. (Birdman, 2011) (Hauri - Response Team, 2011) (Moon-young, 2011) (Jin-woo Seo, 2011)

THE UPDATE SERVER

The update server used by the attackers as a launchpad for their attack against SK Communications was ESTsoft's ALZip update server. ESTsoft is a large South Korean software company and ALZip is a file compression and archive tool developed by the company. ALZip is part of a trusted suite of tools known as ALTools which also includes the antivirus software, ALYac. The antivirus software is independent of the rest of the suite of tools. It uses a different update program and server to the other tools. The security of ALYac was not compromised in the attack. (ESTsoft, 2011) (ESTsoft, 2011)

The attackers, purportedly using Chinese IP addresses[9], gained access to the ALZip update server via unknown means and uploaded instructions to it. Then, when SK Communications computers conducted their routine check for ALTools updates, the attacker's instructions on the update server directed the computers to download a trojaned update from the attacker's Content Delivery Network[10] (CDN) instead of the legitimate update from ESTsoft's CDN. (ESTsoft, 2011)

The trojaned update exploits a software vulnerability[11] in the ALTools Common Module Update Application (ALCMUpdate.exe) - the program used to conduct the routine checks for ALTools software updates. This vulnerability allowed a malicious Dynamic Link Library (DLL)[12] file to be loaded instead of the legitimate DLL update file (ALAd.dll), thereby enabling malicious code to be run and malicious software (malware) to be installed on computers which requested the update. Over 60 SK Communications computers were compromised via the trojaned update. (ESTsoft, 2011) (EDaily, 2011) (ESTsoft, 2011)

The attackers are believed to have designated targets for infection, so that the trojaned update was only delivered to SK Communications computers and not to other computers requesting the same

[5] A vulnerability exists in certain versions of a software program used by SK Communications (amongst other companies) which could allow an attacker to gain control of computers if the program is used on them to open a maliciously crafted file. (Japanese IT Promotion Agency 2011)

[6] According to the Korean National Police Agency the hacker collected information from the infected computers for up to a week before hacking the databases. (Moon-young, 2011)

[7] A 'waypoint' is a computer used by attackers as an intermediary point to obfuscate the source of their hacking activities.

[8] Under South Korea's Real Name System, Koreans were required to submit their real names and resident registration numbers when creating accounts on any website attracting more than 100,000 visitors per day. (TMCnews 2011)

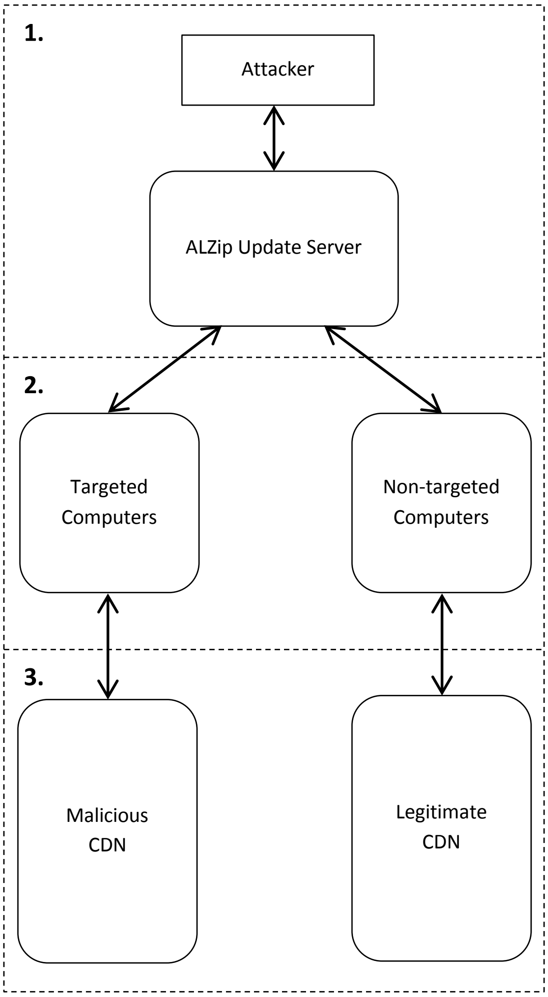
[9] According to South Korean news outlets the attackers used Chinese IP addresses. (Goodin, 2011)

[10] A CDN is comprised of multiple servers which are used to distribute software downloads, thereby balancing the load and preventing outages due to individual servers becoming overloaded.

[11] A software vulnerability existed in the update program used by several tools in the ALTools suite. The vulnerability allowed arbitrary code to be executed but could only be exploited from the actual update server or, if a computer could be directed to it (eg. by modifying the host file on the computer or via DNS hijacking), a fake update server. A patch for the vulnerability was released on 4 August 2011. (ESTsoft 2011) (ESTsoft, 2011)

[12] According to Microsoft, a DLL is a library that contains code and data that can be used by more than one program at the same time. (Microsoft 2007)

software update from the server[13]. The way the update server was used in the attack is depicted in Figure 1.



1. Attacker modifies the ALZip update server.
2. Computers check for ALZip software updates and are redirected to a Content Delivery Network (CDN).
3. Non-targeted computers download a legitimate update from the ESTsoft CDN. Targeted computers download a trojaned update from the attacker's malicious CDN.

FIGURE 1 - DEPICTION OF HOW THE ALZIP UPDATE SERVER WAS USED IN THE ATTACK

This specific targeting of SK Communications indicates the targeting wasn't purely opportunistic. To target the company in the manner they did, the attackers would have needed knowledge of SK Communications and its use of ALZip, ahead of the attack. This knowledge was likely gained during the reconnaissance[14] stage of the attack.

THE INFECTED COMPUTERS

After the ALZip update program (ALCMUpdate.exe) downloaded the trojaned update onto the 60+ SK Communications computers, the computers subsequently became infected with malware known as 'Backdoor.Agent.Hza'. The trojaned update file 'dropped' the malware 'Backdoor.Agent.Hza' onto the computers and, in so doing, gave the attacker a 'backdoor' into them. The trojaned update is detected as 'Trojan.Dropper.Agent.Hza Backdoor.Agent.Hza' and 'V.DRP.Agent.Hza V.BKD.Agent.Hza' by different versions of ESTsoft's ALYac antivirus software. (ESTsoft, 2011) (ESTsoft, 2011)

Once infected, the computers communicated with the command and control server located at South Korean IP address 116.127.121.41 on Transmission Control Protocol (TCP) port 8080[15]. It is possible the infected SK computers used the callback domain 'update.alyac.org' (reportedly associated with the hack[16]) to locate the command and control server. It is, however, unconfirmed whether the domain 'update.alyac.org' resolved to the South Korean IP address at the time of the attack. (ESTsoft, 2011) (Samsung IDC, 2011) (ETnews, 2011)

Between 18 July 2011 and 25 July 2011, the attackers used the infected computers to collect additional internal access information and database credentials. They presumably used a file named 'x.exe'[17] to acquire some of this information, after downloading it onto infected computers from a toolbox they had earlier set up. Based on the behaviour of this file, the attackers likely used it to conduct network enumeration and to obtain

[13] The Korean National Police Agency presumes the hacker, instead of targeting all ALZip users, singled out the intranet computers at SK Communications. (Moon-young, 2011)

[14] For an explanation of the reconnaissance stage of an attack refer to the Command Five Paper 'Advanced Persistent Threats: A Decade in Review' (Command Five Pty Ltd, 2011).

[15] According to Samsung IDC, the ALTools related command and control server was using IP address 116.127.121.41.

[16] According to ETnews the domain 'update.alyac.org' was used in the hack. ETnews does not state how the domain was involved but, given the infected computers had ALTools installed on them, use of 'ALYac.org' in the callback domain may have helped to disguise the malicious communications. (ETnews 2011)

[17] The file named 'x.exe' is 51712 bytes and has a SHA1 hash of 5A1B E6AD CB2C C40B 2E9D 6B6C 569F D4DA B273 E7AD. (JSUNPACK, 2011)

credentials such as usernames and passwords[18]. (Birdman, 2011) (Moon-young, 2011)

The attacker also installed the malware used to access the user databases on at least one of the infected computers. The malware was named 'nateon.exe'[19] and was also hosted on the same toolbox, along with another file named 'rar.exe'[20]. (Birdman, 2011) (Hauri - Response Team, 2011)

Static analysis[21] of the file 'rar.exe' indicates it is a modified version of the WinRar[22] command line program - also named 'rar.exe'. The file may have been used in the attack to create or open archive files. The modifications made to the program remove the program properties from display, presumably to disguise the true nature of the file. This is somewhat redundant in this instance though, given the file name indicates the nature of the program.

THE TOOLBOX

The files downloaded onto the infected SK Communications computers were reportedly hosted at 'www.cph.com.tw/act'[23] – a website belonging to the large Taiwanese publishing company, Cite Media Holding Group[24]. It is likely the company's webserver was compromised unbeknownst to its owner and used by the attacker as a toolbox from which to download malicious files and hacker tools onto targeted computers.

The website 'cph.com.tw' is assumed to have been running on an Internet Information Services (IIS) webserver at the time the server was hacked[25]. IIS runs on the Microsoft Windows operating system, indicating the compromised server was likely running Microsoft Windows. There are a number of known vulnerabilities for both IIS and Microsoft Windows which potentially could have been exploited and resulted in the compromise of the webserver[26].

THE DATABASE ACCESS

After the week collecting information from the infected computers the attackers were ready to access the databases. On 26 July 2011, they used the information they had gathered, along with a malicious program named 'nateon.exe', to access the Nate and CyWorld databases. The theft of information continued into the following day - 27 July 2011. (Birdman, 2011) (Moon-young, 2011) (Hauri - Response Team, 2011)

The personal information extracted from the databases was purportedly sent via a waypoint to a Chinese IP address where the hacker received the information. The waypoint used purportedly belonged to a company based in Seoul's Nonhyeon neighbourhood. (Moon-young, 2011)

The South Korean waypoint may have been located by the malware using the callback domain 'ro.diggfunny.com' which was reportedly associated with the leak of information from the databases[27]. It has not, however, been confirmed whether, at the time of the attack, this callback domain pointed to an IP address belonging to a Nonhyeon-based company.

[18] Antivirus software detects the file as 'Heuristic.BehavesLike.Win32.PasswordStealer.H' and 'HKTL_NETVIEW'. (Hispasec Sistemas, 2011)

[19] The file named 'nateon.exe' is 166912 bytes and has a SHA1 hash of F84C D73D ABF1 8660 7F98 6DF9 8C54 02A5 7BB5 8AD1. It is detected as 'Backdoor.Sogu' by Symantec antivirus software. (JSUNPACK 2011). (Hispasec Sistemas, 2011)

[20] The file named 'rar.exe' is 337920 bytes and has a SHA1 hash of E87C 3ACB A599 5E01 7AD3 1B29 A5E2 FE36 3ED4 D9EB. (JSUNPACK 2011)

[21] Static analysis refers to analysis of a program's code to determine its functionality, as opposed to dynamic analysis in which a program is executed to determine its behaviour.

[22] WinRAR is a popular archiving and compression tool.

[23] The files 'nateon.exe', 'rar.exe' and 'x.exe' were hosted at 'www.cph.com.tw/act'. (Birdman, 2011)

[24] Cite Media Holding Group publishes over 20 million magazine issues each year in Taiwan. (Novell 2011)

[25] An archived error page shows the 'cph.com.tw' website was running on an IIS server in late 2010. (The Internet Archive 2010)

[26] Both the Microsoft Security TechCenter and the US National Vulnerability Database make available a comprehensive list of Microsoft Windows and IIS vulnerabilities. (Microsoft n.d.) (National Institute of Standards and Technology n.d.)

[27] According to Samsung IDC the IP address 116.127.121.109 was associated with the leak of database files from Nate. (Samsung IDC 2011)

```
10026210/10070910: 31 9C 6C 4C  B9 3A 10 00  E8 03 00 00  01 00 50 00  1.lL.:..è.....P.
10026220/10070920: 6E 61 74 65  6F 6E 2E 64  75 61 6D 6C  69 76 65 2E  nateon.duamlive.
10026230/10070930: 63 6F 6D 00  00 00 00 00  00 00 00 00  00 00 00 00  com.............
10026240/10070940: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
…
100268A0/10070FA0: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
100268B0/10070FB0: 00 00 00 00  00 00 00 00  00 00 00 00  77 69 6E 73  ............wins
100268C0/10070FC0: 76 63 66 73  00 00 00 00  00 00 00 00  00 00 00 00  vcfs............
100268D0/10070FD0: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
…
10026930/10071030: 00 00 00 00  00 00 00 00  00 00 00 00               ............
```

FIGURE 2 - EXCERPTS FROM THE 'NATEON.EXE' CONFIGURATION BLOCK

THE DESTORY RAT

Structure and Behaviour

The malicious program named 'nateon.exe' installs a Remote Administration Tool (RAT) named 'winsvcfs.dll'. It modifies the system registry in such a way that the RAT gets executed as a service by the trusted process 'svchost.exe'[28] each time the computer is started. Once 'winsvcfs.dll' is installed, 'nateon.exe' is deleted. Both 'nateon.exe'[29] and 'winsvcfs.dll'[30] are now detected by some antivirus software.

Static analysis of the malware reveals a configuration block. This configuration block contains the name of the DLL file which 'nateon.exe' is to create. In this instance, the configured named was 'winsvcfs.dll', as shown in Figure 2. Due to the name being configurable, the RAT will not always be called 'winsvcfs.dll'. The configuration block also contains a callback domain and port for the malware's command and control communications. The callback domain is configured to be 'nateon.duamlive.com' and the port is configured to be 80 (50 in hexadecimal), also shown in Figure 2.

If no configuration is specified, the malware uses default values instead. The default callback location hardcoded into the malware is the private IP address, 192.168.0.200. This address is not routable on the Internet and suggests the attackers rely on the configuration instead of the hardcoded callback address.

According to information contained within 'nateon.exe', the malware used in the SK Communications hack was compiled from source code on 27 September 2010 at 01:17.04 - over 6 months before the attack. The configuration block was likely inserted into the binary after this date as the callback domain was not registered until May 2011. This may indicate that the RAT has been used in other attacks but with different configurations. If the previously identified 'Backdoor.Sogu'[31] is a version of the malware, other callback domains previously configured may include those known to be used by 'Backdoor.Sogu'. These domains include 'bbs.afbjz.com', 'newhose.ntimobile.com', and 'www.adv138mail.com'[32].

The RAT has many different capabilities and runs on multiple versions of the Microsoft Windows operating system. The RAT's behaviour changes slightly depending on which version of the Windows operating system it is installed on and which modules are installed. Modules used by the RAT deployed to the SK Communications network include:

[28] The process 'svchost.exe' is a generic host process for services which run from DLLs. (Microsoft, A description of Svchost.exe in Windows XP Professional Edition 2007)

[29] On 29 July 2011, 23 of 43 antivirus products tested detected 'nateon.exe' as malware, as of 19 August 2011 this number had increased to 36 of the 43. (Hispasec Sistemas 2011) (Hispasec Sistemas 2011)

[30] As of 6 September 2011, 34 of 44 antivirus products tested detected 'winsvcfs.dll' as malware. (Hispasec Sistemas 2011)

[31] Symantec antivirus software detects 'nateon.exe' as 'Backdoor.Sogu'. The malware described by Symantec exhibits similar behaviour to 'nateon.exe' but is a smaller size. (Mullaney, 2011)

[32] In addition to being used by 'Backdoor.Sogu', the callback domain 'www.adv138mail.com' was used by a Poison Ivy RAT in a July 2011 socially engineered email campaign which targeted experts on the relationship of the United States with Japan, China and Taiwan. (Parkour, 2011)

- advapi32.dll,
- cryptbase.dll,
- gdi32.dll,
- iphlpapi.dll,
- kernel32.dll,
- mpr.dll,
- msvcrt.dll,
- ntdll.dll,
- odbc32.dll,
- ole32.dll,
- psapi.dll,
- sfc.dll,
- shell32.dll,
- shlwapi.dll,
- user32.dll,
- userenv.dll,
- version.dll,
- wininet.dll,
- ws2_32.dll,
- wtsapi32.dll.

Of note, the module 'odbc32.dll' is used in the access of databases. The RAT uses a number of Standard Query Language (SQL)[33] functions which are accessed (or more technically, dynamically imported) as the software runs. These include:

- SQLAllocHandle,
- SQLColAttributeW,
- SQLDisconnect,
- SQLDriverConnectW,
- SQLExecDirectW,
- SQLFetch,
- SQLFreeHandle,
- SQLGetData,
- SQLGetDiagRecW,
- SQLMoreResults,
- SQLNumResultCols,
- SQLSetEnvAttr.

These functions would have been utilised by the attacker to communicate with the Nate and CyWorld user databases and thereby, to obtain the personal details.

The RAT can not only access and query databases but can also enumerate the networks to which the infected computer is connected, set up network connections, modify the registry, lock the workstation's screen, control processes and services running on the computer, download files, create files, take screenshots and shutdown, reboot or log out of the computer. The RAT has four different operating modes; SMI (Install), SMU (Uninstall), SMRAC (Run as Console) and SMRACU (Run as Console User). (Hauri - Response Team, 2011)

A complete list of strings obtained through static analysis of the malware is provided in Annex A. These strings give additional insight into the RAT and its behaviour. Of note, a unique string is present which may be used to associate 'nateon.exe' with other malware. This string is 'CONFIG DESTORY!' and is contained within the malware in an obfuscated form. The string is displayed in a pop-up window if an integrity check the malware performs on its configuration fails.

The RAT employs some basic obfuscation techniques. All strings are obfuscated in memory and only decoded when they need to be used, thereby making static analysis more difficult. In addition, unnecessary operations are inserted at frequent intervals throughout the code. The prolific use of unnecessary operations is likely to make reverse engineering more difficult and potentially indicates that the malware is polymorphic[34]. The RAT, while in some ways sophisticated, still hides in plain sight – limiting its scope for obfuscation.

Communications

The RAT attempts communications to a command and control server located using a callback domain. It also creates a raw socket and binds it to the infected computer's local IP address (as assigned to the computer's network interface card). This is not, however, for the RAT to accept inbound connection requests. The socket is configured by the RAT in such a way that it acts as a packet sniffer, whereby, the RAT receives a copy of all inbound and outbound network traffic on the bound interface. As well as enabling deep inspection of this network traffic, the capability could allow the RAT to passively receive commands on any port using any protocol.

Before attempting communications to the command and control server, the malware checks for network connectivity. It does this by using the

[33] SQL instructions are used to query certain types of databases and obtain information from them.

[34] Polymorphic programs can be modified (or modify themselves) to have a different file hash and/or size while retaining the same functionality. This facilitates code reuse by making signature based detection more difficult.

legitimate Microsoft Windows domain 'download.windowsupdate.com'. This legitimate domain is hardcoded into the malware but may be overridden by modifying the malware's configuration.

Having determined there is network connectivity, the malware establishes communications with the callback domain 'nateon.duamlive.com'[35] on TCP port 80 (configured as noted previously). Communications occur over the HyperText Transfer Protocol (HTTP) protocol – a protocol commonly used on TCP port 80 for website browsing. The malware appears to be proxy-aware and capable of communicating via a web proxy.

The following malformed user-agent[36] is present in the HTTP requests (spaces shown here as '·'): 'Mozilla/4.0·(compatible;·MSIE·6.0;·Windows·NT·5.1;SV1;'.

This user-agent is consistent with that which may be expected from a user running version 6.0 of the Microsoft Internet Explorer web browser on the Microsoft Windows XP operating system, except that it is missing a closing bracket after the last semicolon and a space after the second to last semicolon. This malformed user-agent is hardcoded and can be used as a signature to detect HTTP communications produced by the malware.

Four custom headers are also present in the HTTP requests: 'X-Session', 'X-Status', 'X-Size', and 'X-Sn'. The file path requested is '/update?product=windows'. These custom headers and the file path may also be used to develop signatures for detection of the RAT's communications.

Once the malware successfully contacted the command and control server, the attacker would have been able to give it instructions to access the Nate and Cyworld databases and to send data from them back to a location the attacker could access.

The name of the malware and the name of the selected callback domain were presumably chosen by the attackers to disguise them as being associated with NateOn - an Instant Messaging Service owned by SK Communications. Legitimate files developed by SK Communications are also known by the name 'nateon.exe'[37].

The Malicious Infrastructure

Callback domains are translated to IP addresses using the Domain Name System (DNS)[38] protocol. This translates the domain into a unique address on the Internet which infected computers can use to locate and communicate with a command and control server. Command and control servers are typically more resource intensive to set up and maintain than callback domains which may be used to direct communications to them. It is not uncommon for multiple domains to identify the same command and control infrastructure.

In late July 2011, at the time of the attack, the callback domain 'nateon.duamlive.com' pointed to the South Korean IP address 121.78.237.135 but at the time of writing points to local loopback IP address 127.0.0.1[39]. Attackers quite commonly point a callback domain to a local loopback IP address when they do not have any instructions for the infected computers using that domain. This prevents the computers from unnecessarily contacting the attacker's command and control infrastructure. Attackers also quite commonly point a callback domain to a local loopback IP address when they want to protect their command and control infrastructure from detection.

At the time of the attack, the callback domain 'ro.diggfunny.com' pointed to the South Korean IP address 116.127.121.109. This IP address is in the same IP address range (116.127.0.0/16) [40] as the IP address used by the ALTools related command and control server (IP address 116.127.121.41). The IP

[35] Multiple sources confirm the malware used in the hack called back to 'nateon.duamlive.com'. (Samsung IDC 2011) (Birdman, 2011)

[36] User-agents are used in HTTP communications to tell webservers which operating system and web browser their clients are using, so they can serve compatible webpages.

[37] Different versions of a legitimate file named 'nateon.exe' exist. These files are associated with the NATEON Upgrader developed by SK Communications. (Mister Group n.d.)

[38] DNS is fundamental on the Internet. It is a form of directory assistance to help computers communicate with other computers. Its use is analogous to a person calling directory assistance to find out what phone number to dial to speak to a certain person.

[39] A local loopback IP address is an address which is not Internet or Intranet routable, ie. it can not be used by a computer to communicate with another computer. When a computer attempts to communicate with a local loopback IP address, it communicates with itself.

[40] The IP address range 116.127.0.0/16 is the Classless Inter-Domain Routing (CIDR) representation of IP addresses 116.127.0.0 through 116.127.255.255.

address range is allocated to the South Korean ISP Hanaro Telecom.

A portion of the IP address range appears to have been assigned by Hanaro Telecom to a South Korean web hosting company. It is not known whether the two IP addresses used by the attackers fall within the range used by the webhosting company. It is also unconfirmed whether that company is based in Nonhyeong - the geographic region of the company that hosted the waypoint used in the attack.

If the IP addresses used by the attackers in the range 116.127.121.0/24 were assigned to the web hosting company, it is possible the attackers purchased webhosting services through the company to host their command and control servers instead of compromising legitimate servers. Other IP addresses in the range are also associated with malware[41] but that malware may not be related in any way to the SK Communications hack or the attackers involved in the hack.

In late July 2011, at around the time of the attack, the callback domain 'update.alyac.org' pointed to the South Korean IP address 202.30.224.240. As at the time of writing, the domain now points to the legitimate Google IP address 8.8.8.8. This is not an indication that the Google IP address is compromised, and the Google IP address is unlikely to be compromised.

The Google IP address is likely only used to indicate that the attacker has no instructions for the malware or to instruct the malware to continue with pre-programmed behaviour. The malware likely has logic built in which prevents it from communicating with the Google IP address. Use of the Google IP address would likely achieve the attacker's desired outcome in a similar way to use of a local loopback IP address. It would, however, be less likely to flag the activity to network defenders[42].

It is also possible the Google IP address is used to channel covert communications to the command and control server over the DNS protocol[43], in effect, using Google as a voluntary waypoint without actually compromising Google's infrastructure.

Each of the three callback domains has a Time-To-Live (TTL)[44] of 30 minutes, allowing the attackers to rapidly change the command and control server pointed to by the callback domain.

Registration Information

The domain 'duamlive.com' was registered on 21 May 2011. It was registered by a 'Guangming Wang'. There is a large number of domain registrations (approximately 400) associated with 'Guangming Wang', possibly indicating that the domains were registered by an intermediary.

The domain 'alyac.org' was registered on 24 September 2010. The domain registration information is almost identical to that of the legitimate ESTsoft domain 'alyac.com'. The domain is not, however, associated with the ALYac antivirus software and does not appear to be associated with ESTsoft at all. The title of the website previously hosted at 'alyac.org' was associated with finance, insurance and cell phones and not antivirus software[45].

At the time of writing, the malicious domain 'alyac.org' points to the Google IP address 8.8.8.8 but previously pointed to South Korean IP address 222.122.20.241. Other probable malicious domains following a similar pattern to 'alyac.org' (whereby they disguise themselves as being associated with legitimate software companies) have also pointed to the same South Korean IP address. These include the domains 'trendmicros.net', 'nprotects.org' and 'bomuls.com'.

The domain 'trendmicros.net' was purportedly registered by Trend Micro Inc. The registration details are almost identical to that of the legitimate domain 'trendmicro.com'. The domain, however, appears to have nothing to do with the security company. The malicious domain 'nprotects.org' is similar to that of the legitimate security company

[41] The command and control servers of dozens of pieces of malware have used IP addresses within the IP address range 116.127.121.0/24. (Malc0de.com n.d.)

[42] Use of legitimate IP addresses in combination with preprogramed logic to prevent a communication with command and control infrastructure is a much less common indicator of malicious activity than use of a local loopback IP address for the same purpose.

[43] The malware could use a similar technique to software such as iodine. (Kryo, 2010)

[44] The TTL of a domain in a DNS record refers to the duration for which the DNS result can be cached.

[45] A webpage previously hosted at 'alyac.org' had a title of 'Cash Advance | Debt Consolidation | Insurance | Free Credit Report | Cell Phones at alyac.org'. (Domain Tools, LLC, 2011)

nProtect ('nprotect.com') but again, does not appear to be associated with the company. The domain has previously been associated with malware known as 'Trojan.Win32.Generic' [46]. Similarly the domain 'bomuls.com' is not dissimilar to that of the legitimate software company whose website resides at 'bomul.com'. (ETnews, 2011)

The domains referenced above are summarised in Table 1.

DOMAIN	SUBDOMAIN	IP ADDRESS(ES)
DUAMLIVE.COM	-	127.0.0.1*
	NATEON.	121.78.237.135 (KR) 127.0.0.1*
	FR.	121.78.237.135 (KR) 127.0.0.1*
ALYAC.ORG	-	222.122.20.241 (KR) 8.8.8.8 (US)*
	UPDATE.	202.30.224.240 (KR) 8.8.8.8 (US)*
	PATH.	8.8.8.8 (US)*
	WWW.	8.8.8.8 (US)*
NPROTECTS.ORG	-	222.122.20.241 (KR)*
	FILE1.	222.122.20.241 (KR)*
	PC.	220.90.209.157 (KR) 222.122.20.241 (KR)*
TRENDMICROS.NET	-	222.122.20.241 (KR)*
	DOWNLOAD.	222.122.20.241 (KR)*
	BBS.	222.122.20.241 (KR)*
BOMULS.COM	-	66.249.89.104 (US) 222.122.20.241 (KR) 98.126.8.230 (US)*
	DOWNLOAD.	222.122.20.241 (KR)*
	FORUM.	222.122.20.241 (KR)*

* Indicates IP address assigned at time of writing.

TABLE 1 - SUMMARY OF REFERENCED DOMAINS

The domain 'diggfunny.com' was registered on 14 April 2011 by a 'Lee Cooper'. The same registrant details were used to register several other domains. These domains include 'edsplan.com', 'ezxsoft.com', 'finalcover.com', 'mindplat.com', 'projectxz.com', and 'soucesp.com' - all of which were registered on 14 April 2011. The domains 'daumfan.com' and 'natefan.com' were also registered by 'Lee Cooper', but on 25 July 2011, the day before the hacking operation against the Nate and CyWorld user databases. The same registrant details were purportedly used to register an additional seven domains. Each of these domains has a TTL of 30 minutes. (Domain Tools, LLC, 2011)

At the time of writing none of the above domains registered by 'Lee Cooper' point to a malicious IP address. The domain 'natefan.com' points to the Google IP address 8.8.8.8, 'daumfan.com' points to the Enom Inc[47] IP address 8.5.1.42, 'finalcover.com' points to the private IP address 192.168.10.132 and none of 'diggfunny.com', 'ezxsoft.com', 'edsplan.com', 'mindplat.com', 'projectxz.com' or 'soucesp.com' currently point to an IP address. This suggests the domains are not currently in use, however, at least one subdomain appears to be in current use as shown in Table 2.

[46] Malware detected as 'Trojan.Win32.Generic' in May 2011 used the callback domain 'pc.nprotects.org'. (GFI SandBox, 2011)

[47] Enom Inc is a legitimate domain name registrar used by the attackers to register domain names and also to host webpages.

Domain	Subdomain	IP address(es)
DAUMFAN.COM	-	8.5.1.8 (US) 8.5.1.42 (US)*
	WWW.	8.5.1.8 (US) 8.5.1.42 (US)*
DIGGFUNNY.COM	-	8.8.8.8 (US)
	RO.	116.127.121.109 (KR)
	WWW.	8.8.8.8 (US) 61.19.250.219(TH)
EDSPLAN.COM	-	64.74.223.10 (US)
	ITT.	127.0.0.1*
EZXSOFT.COM	-	
	BBS.	202.30.224.240 (KR) 8.8.8.8* (US)
FINALCOVER.COM	-	192.168.10.132*
	I.	69.197.132.132 (US) 127.0.0.1*
	T.	218.213.229.69 (HK) 218.213.229.68 (HK)*
MINDPLAT.COM	-	64.74.223.48 (US)
	CACHE.	8.8.8.8 (US)*
NATEFAN.COM	-	8.8.8.8 (US)*
PROJECTXZ.COM	-	8.5.1.11 (US)
	ITT.	202.181.170.67 (HK) 8.8.8.8 (US)*
SOUCESP.COM	-	61.82.71.30 (KR) 127.0.0.1

* Indicates IP address assigned at time of writing.

TABLE 2 - DOMAINS REGISTERED BY LEE COOPER

Several of the domains registered by 'Lee Cooper' previously pointed to webpages. The domain 'mindplat.com' previously pointed to an Enom Inc. server which hosted its webpage. The title and meta description of the 'mindplat.com' website is almost identical to that of the 'alyac.org' website. Both websites follow the template shown in Figure 3. The same template has also been used for several other webpages and may merely be a template provided by a service provider used by the registrants.

The domains 'natefan.com' and 'projectxz.com' also previously pointed to webpages. The webpages were similar to the 'mindplat.com' and 'alyac.org' webpages but with different text. Again, these webpages use the same template as other webpages and may merely be provided by a service provider. The presence of these webpages may indicate an attempt by the attackers to make the malicious domains appear more legitimate.

Title

Cash Advance | Debt Consolidation | Insurance | Free Credit Report | Cell Phones @ *domain*

Meta Description

Find Cash Advance, Debt Consolidation and more at *domain*. Get the best of Insurance or Free Credit Report, browse our section on Cell Phones or learn about Life Insurance. *Domain* is the site for Cash Advance.

FIGURE 3 - EXAMPLE OF WEBPAGE TEMPLATE USED

SIMILARITIES TO OTHER MALWARE

As previously discussed, the domain 'ro.diggfunny.com' is associated with malicious activity. The domains 'cache.mindplat.com' and 'bbs.ezxsoft.com' are also known to be associated with malware. The first is listed as a malicious domain[48] and the second was used as a callback domain by malware known as 'Trojan.Win32.AgentBypass' [49] . The domain 'bbs.ezxsoft.com' also previously pointed to the same South Korean IP address as 'update.alyac.org' (IP address 202.30.224.240), further linking it to the attackers responsible for the hack into SK Communications.

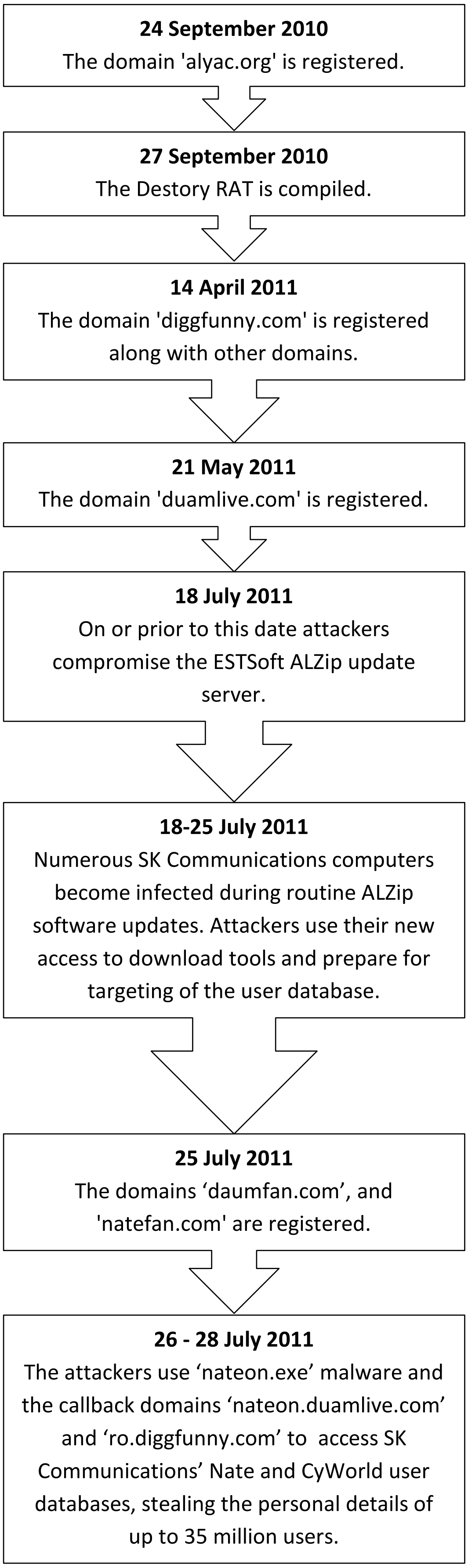
Even if ignoring the connection they both have to the domain 'alyac.org', the two pieces of malware named 'Trojan.Win32.Generic' and 'Trojan.Win32.AgentBypass' respectively (earlier referenced) are still linked. Both pieces of malware create a uniquely named directory[50], as do at least three other pieces of malware (summarised in Annex B). This further links the domains 'nprotects.org' and 'ezxsoft.com', and suggests this malware, along with the callback domains, may be part of a broader, concerted effort by the same attackers.

[48] The domain 'cache.mindplat.com' is listed alongside 'ro.diggfunny.com' in a list of malicious web addresses. (CEOinIRVINE 2011).

[49] Malware detected as 'Trojan.Win32.AgentBypass' in mid July 2011 used the callback domain 'bbs.ezxsoft.com'. (GFI SandBox 2011)

[50] Malware analysis reports indicate both pieces of malware create a directory named '03a075fb70d5d675f9dc26fc' inside the system directory and a subdirectory named 'update'. (GFI SandBox 2011) (GFI SandBox, 2011)

Timeline



24 September 2010
The domain 'alyac.org' is registered.

27 September 2010
The Destory RAT is compiled.

14 April 2011
The domain 'diggfunny.com' is registered along with other domains.

21 May 2011
The domain 'duamlive.com' is registered.

18 July 2011
On or prior to this date attackers compromise the ESTSoft ALZip update server.

18-25 July 2011
Numerous SK Communications computers become infected during routine ALZip software updates. Attackers use their new access to download tools and prepare for targeting of the user database.

25 July 2011
The domains ‘daumfan.com’, and 'natefan.com' are registered.

26 - 28 July 2011
The attackers use ‘nateon.exe’ malware and the callback domains ‘nateon.duamlive.com’ and ‘ro.diggfunny.com’ to access SK Communications’ Nate and CyWorld user databases, stealing the personal details of up to 35 million users.

Insights

- Attackers will conduct reconnaissance on their targets and consider all sorts of targeting options (both direct and indirect).
- Attackers may target a company in order to use it as a ‘launchpad’ to gain access to other targets, as demonstrated by the targeting of ESTsoft's ALZip update server.
- Attackers can conduct selective targeting - choosing which computers download malicious content and which do not, as they appear to have done with the ALZip update server.
- Even though two computers may submit an identical request for a file (or webpage), they may not get the same file (or webpage) back in response. This behaviour reduces the likelihood of malware unintentionally going viral. Unfortunately it also hampers investigations by network defenders who may assess a file (or webpage) to be safe, when it is not safe to all users.
- Attackers may hack a computer for the sole purpose of using it as a ‘waypoint’ or as an intermediary location from where they can store and access their tools without suspicion from their targets. This appears to have been the case with the use of the Cite Media Holding Group webserver and the Nonhyeong based waypoint, although it is possible they were initially hacked for another reason.
- Attackers may use the same registration information to register multiple domain names. Such appears to have been the case with the domains registered by ‘Lee Cooper’.
- Attackers may register domains containing words that are expected to make them appear less suspicious to targets. Such as with the use of ‘nateon'and ‘alyac’ in the callback domains used by infected SK Communications computers.
- Attackers may use seemingly legitimate registration information to register domain names. Such appears to have been the case with the registration of ‘alyac.org’ and ‘trendmicros.net’.
- Users should be wary of domains which appear to be legitimate but are not. Such as ‘alyac.org’ instead of ‘alyac.com’,

‘trendmicros.net’ instead of ‘trendmicro.com’, ‘nprotects.org’ instead of ‘nprotect.com’ and ‘bomuls.com’ instead of ‘bomul.com’.

- Even though it is relatively easy to create new infrastructure, attackers sometimes reuse infrastructure. For example, the domains ‘bbs.ezxsoft.com’ and ‘update.alyac.org’ both previously pointed to IP address 202.30.244.240, and ‘alyac.org’, ‘trendmicros.net’, ‘nprotect.org’ and ‘bomuls.com’ all pointed to IP address 222.122.20.241.
- The TTL of domains (in DNS records) controlled by attackers are often set to low values (such as 30 minutes) allowing the attackers to rapidly change the command and control server pointed to by a callback domain. This facilitates relatively uninterrupted access to a target when command and control infrastructure becomes blocked or is otherwise unavailable.
- The use of legitimate domains for malicious purposes, familiar words in domain names and of non-malicious IP addresses in DNS records for malicious domains, can make detection of malicious activity more difficult and cause network defenders to dismiss malicious activity (in network/system logs or Intrusion Detection System alerts, in particular) as legitimate.
- Adding malicious IP addresses and domains to blacklists can help prevent malicious activity, however, attackers can respond by merely using alternate infrastructure and/or callback domains.
- Domains and IP addresses may have legitimate purposes too and blacklisting them may also block legitimate business. Blacklists should be reviewed periodically to ensure they are not blocking legitimate business unnecessarily.
- Whitelists are generally much more effective than blacklists, however, even whitelists can allow malicious activity to occur to legitimate sites that have been compromised. For example, as a good security practice, most system administrators would have allowed access to the ALZip update server if they had ALZip software installed on their network. Similarly, if a whitelist were employed on the targeted network but users had a legitimate need to access the website of the Taiwanese publishing company, the attacker would likely still have been able to access their toolbox.
- Users and network administrators need to continually reassess who and what they trust on the Internet given that trust relationships can be, and increasingly are, exploited for malicious purposes.

Disclaimer

Machine translation software has been heavily relied on throughout the development of this paper. While data has been verified against multiple sources, where possible, Command Five Pty Ltd does not guarantee the veracity of sources or the accuracy of translation and interpretation. Command Five Pty Ltd reminds readers to exercise caution when visiting untrusted websites and/or opening untrusted digital documents. Command Five Pty Ltd does not warrant that the websites referenced in this paper are trustworthy.

REFERENCES

Birdman. (2011, July 31). *Xecure Lab Blog*. Retrieved August 12, 2011, from http://blog.xecure-lab.com/2011/07/2500.html

CEOinIRVINE. (2011, August 17). *Information Security & US & Life & Love & Fashion & Hacking & Passion*. Retrieved September 13, 2011, from http://hack3r.tistory.com/tag/Malware

Command Five Pty Ltd. (2011, June). *Advanced Persistent Threats: A Decade in Review.* Retrieved September 24, 2011, from Command Five Pty Ltd: http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf

Domain Tools, LLC. (2011). *AlYAc.org - Al Y Ac - Screenshot History*. Retrieved September 08, 2011, from DomainTools: http://www.domaintools.com/research/screenshot-history/alyac.org

Domain Tools, LLC. (2011). *Reverse Whois Lookup | Domain Ownership Search | Domain Tools*. Retrieved September 22, 2011, from Domain Tools: http://www.domaintools.com/research/reverse-whois/?all[]=leecooper%40korea.com&none[]=

EDaily. (2011, August 11). *Nate hack related.* Retrieved September 14, 2011, from EDaily Korean News: http://www.edaily.co.kr/news/NewsRead.edy?SCD=DC16&newsid=02056566596346336&DCD=A01405&OutLnkChk=Y

ESTsoft. (2011, August 04). *ESTsoft apology for ALTools security vulnerability.* Retrieved September 14, 2011, from ESTsoft Blog: http://blog.estsoft.co.kr/138

ESTsoft. (2011, August 05). *ESTsoft news release with respect to ALTools security vulnerability.* Retrieved September 19, 2011, from ESTsoft Blog: http://blog.estsoft.co.kr/139

ESTsoft. (2011, August 11). *Police release interim results on Nate hack.* Retrieved September 14, 2011, from ESTsoft Blog: http://blog.estsoft.co.kr/143

ESTsoft. (2011, August 04). *Urgent security patches for public ALTools products.* Retrieved September 20, 2011, from ALTools Announcements: http://www.altools.co.kr/Plaza/Notice_Contents.aspx?idx=828

ETnews. (2011, August 05). *ETnews - Nate hack, planned since last year?* Retrieved August 12, 2011, from http://www.etnews.com/news/print.html?id=201108050128

GFI SandBox. (2011, May 30). *GFI SandBox Malware Analysis Report: Backdoor.Win32.Generic*. Retrieved September 22, 2011, from GFI SandBox: http://xml.ssdsandbox.net/view/6c6adbd087276ae89f8262582798b708

GFI SandBox. (2011, July 15). *GFI SandBox Malware Analysis Report: Trojan.Win32.AgentBypass*. Retrieved August 25, 2011, from http://xml.ssdsandbox.net/view/fdf2c5c2b1874efe7fd335092df2d3bc

GFI SandBox. (2011, May 29). *GFI SandBox Malware Analysis Report: Trojan.Win32.Generic!SB Trojan.Trojan.Win32.Generic*. Retrieved September 2011, 2011, from http://xml.ssdsandbox.net/view/bce1069dd099f15170c5fd05bae921b5

GFI Software. (2011, February 08). *CWSandbox Report By MD5 at Sunbelt Security*. Retrieved September 22, 2011, from http://www.sunbeltsecurity.com/partnerresources/cwsandbox/md5.aspx?id=e8ee9373ee6c836042e8f48d8de2dda9

Goodin, D. (2011, August 12). *Software maker fingered in Korean hackocalypse.* Retrieved September 06, 2011, from The Register: http://www.theregister.co.uk/2011/08/12/estsoft_korean_megahack/

Hauri - Response Team. (2011, August 04). *SK Communications detailed analysis report of nateon.exe malware*. Retrieved August 12, 2011, from http://www.hauri.co.kr/updata/SK_detail_report.pdf

Hispasec Sistemas. (2011, September 06). *VirusTotal*. Retrieved September 22, 2011, from http://www.virustotal.com/file-scan/report.html?id=727c5a2c3db079351a79351a79367a1d9eada072a8e19bce0a02eb680088e8eae9bd67-1315308204

Hispasec Sistemas. (2011, August 03). *VirusTotal - Free online Virus, Malware and URL Scanner*. Retrieved August 12, 2011, from http://www.virustotal.com/file-scan/report.html?id=74455d5e8f99272aec64bce106b1e8ff39a122a7d27d362a274af31ab5a4fb1e-1313643321

Hispasec Sistemas. (2011, August 19). *VirusTotal - Free Online Virus, Malware and URL Scanner*. Retrieved September 22, 2011, from http://www.virustotal.com/file-scan/report.html?id=74455d5e8f99272aec64bce106b1e8ff39a122a7d27d362a274af31ab5a4fb1e-1313760695

Hispasec Sistemas. (2011, July 29). *VirusTotal - Free Online Virus, Malware and URL Scanner*. Retrieved September 22, 2011, from http://www.virustotal.com/file-scan/report.html?id=74455d5e8f99272aec64bce106b1e8ff39a122a7d27d362a274af31ab5a4fb1e-1311902003

Hispasec Sistemas. (2011, August 07). *VirusTotal - Free Online Virus, Malware and URL Scanner*. Retrieved August 18, 2011, from http://www.virustotal.com/file-scan/report.html?id=b6aecab3c07e915e27db4b4be4c32de1ffa613029818bbd1bb755653c10fbe38-1311920836

Japanese IT Promotion Agency. (2011, June 29). *IPA/ISEC: Vulnerabilities: Security Alert for Vulnerability in ALZip.* Retrieved September 18, 2011, from Japanese IT Promotion Agency: http://www.ipa.go.jp/security/english/vuln/201106_alzip_en.html

Jin-woo Seo, J.-h. H. (2011, July 28). *35mn User Info Leaked in Cyber Attack against S. Korean Portals.* Retrieved September 19, 2011, from MK Business News: http://news.mk.co.kr/english/newsRead.php?sc=30800005&cm=General&year=2011&no=491540&selFlag=sc&relatedcode=&wonNo=&sID=308

JSUNPACK. (2011, July 27). *jsunpack - a generic JavaScript unpacker*. Retrieved August 14, 2011, from http://jsunpack.jeek.org/dec/go?report=9f5addc7e0c7c57eab347ba10e9a81a032cf0daf

JSUNPACK. (2011, July 27). *jsunpack - a generic JavaScript unpacker*. Retrieved August 08, 2011, from http://jsunpack.jeek.org/dec/go?report=f84cd73dabf186607f986df98c5402a57bb58ad1

JSUNPACK. (2011, July 27). *jsunpack - a generic JavaScript unpacker*. Retrieved August 04, 2011, from http://jsunpack.jeek.org/dec/go?report=2c645b8dee2789a0d5d1c1e173ca3bb6b0d0528e

Kryo. (2010, February 6). *kryo.se: iodine (IP-over-DNS, IPv4 over DNS tunnel)*. Retrieved September 18, 2011, from kryo.se: http://code.kryo.se/iodine

Malc0de.com. (n.d.). *116.127.121 | Malc0de Database.* Retrieved August 22, 2011, from Malc0de Database: http://malc0de.com/database/index.php?search=116.127.121&IP=on

Microsoft. (2007, December 10). *A description of Svchost.exe in Windows XP Professional Edition.* Retrieved September 07, 2011, from Microsoft Support: http://support.microsoft.com/?kbid=314056

Microsoft. (2007, December 04). *What is a DLL?* Retrieved September 18, 2011, from Microsoft Support: http://support.microsoft.com/kb/815065

Microsoft. (n.d.). *Security Center - Bulletins Advisories Tools Guidance Resources.* Retrieved September 09, 2011, from Microsoft Security TechCenter: http://technet.microsoft.com/en-us/security/default

Mister Group. (n.d.). *nateon.exe - What is the nateon.exe?* Retrieved September 06, 2011, from http://systemexplorer.net/db/nateon.exe.html

Moon-young, L. (2011, August 12). *Personal information hack traced to Chinese IP address.* Retrieved September 09, 2011, from The Hankyoreh Media Company: http://english.hani.co.kr/arti/english_edition/e_national/491514.html

Mullaney, C. (2011, July 30). *Backdoor.Sogu Technical Details | Symantec*. Retrieved August 18, 2011, from http://www.symantec.com/security_response/writeup.jsp?docid=2011-073003-5345-99

National Institute of Standards and Technology. (n.d.). *National Vulnerability Database*. Retrieved September 20, 2011, from http://nvd.nist.gov/home.cfm

Novell. (2011). *Novell Customer: Cite Media Holding Group*. Retrieved July 29, 2011, from http://www.novell.com/success/cite.html

Parkour, M. (2011, July 14). *contagio: Jul 13 CVE-2010-2883 PDF Meeting Agenda with more Poison Ivy www.adv138mail.com | 112.121.171.94.* Retrieved September 22, 2011, from Contagiodump Blog: http://contagiodump.blogspot.com/2011/07/jul-13-cve-2010-2883-pdf-meeting-agenda.html

Samsung IDC. (2011, August 05). *Samsung IDC Helpdesk Notice*. Retrieved August 12, 2011, from http://www.samsungidc.com/helpdesk/notice_view.jsp?bpd_seq=0000001532

SK Communications. (n.d.). *SK Communications - About Us*. Retrieved September 06, 2011, from http://corp.skcomms.co.kr/eng/global.htm

Sung-jin, Y. (2011, July 28). *35m Cyworld, Nate users' information hacked.* Retrieved September 06, 2011, from Korea Herald: http://www.koreaherald.com/lifestyle/Detail.jsp?newsMLId=20110728000881

The Internet Archive. (2010, August 14). *Error page.* Retrieved September 18, 2011, from The Internet Archive Wayback Machine: http://web.archive.org/web/20100814135834/http://www.cph.com.tw/1jebugldgJtOAjb1wnXe8A==

ThreatExpert. (2011, July 13). *ThreatExpert Report: Trojan.Win32.Scar.dysk, Bat/sdel*. Retrieved September 22, 2011, from http://www.threatexpert.com/report.aspx?md5=16a31aa8e7ddf66a31551840573b6575

ThreatExpert. (2011, August 03). *ThreatExpert Report: Trojan.Win32.Scar.dzoc*. Retrieved September 22, 2011, from http://www.threatexpert.com/report.aspx?md5=bce1069dd099f15170c5fd05bae921b5

ThreatExpert. (2011, July 29). *ThreatExpert Report: Virus.Win32.Virut*. Retrieved September 22, 2011, from http://www.threatexpert.com/report.aspx?md5=aba9baea70825e6adf0723587f273dc4

TMCnews. (2011, August 11). *S. Korea plans to scrap online real-name system.* Retrieved September 19, 2011, from TMCnews: http://www.tmcnet.com/usubmit/2011/08/11/5698912.htm

ANNEX A

LIST OF DEOBFUSCATED STRINGS FOUND WITHIN ‘NATEON.EXE’

Strings inside ‘nateon.exe’ are stored in an obfuscated form and only deobfuscated as, and while, they are needed. This table contains a complete list of deobfuscated strings extracted during static binary analysis of the malicious file. For each string, two addresses are provided – the ‘Code Address’ and the ‘Obfuscated Address’. The ‘Code Address’ is the address, in code, from which the string deobfuscation is requested. This address can be used to efficiently identify wrapper functions that dynamically import system APIs (such as those used for network communications), as well as to locate interesting parts of the malware. The ‘Obfuscated Address’ is the address, in data, where the obfuscated string is stored.

For readability, the strings presented in the ‘Deobfuscated String’ column have been converted from their original formats. Some of the strings are stored inside ‘nateon.exe’ as 8-bit character strings and some as 16-bit wide character strings. Non-printable characters have been escaped as hexadecimal values in the form ‘<\xHH>’ or ‘<\uHHHH>’. Trailing null (‘<\x00>’) characters are not shown. Standard escape sequences such as ‘\n’ (newline) and ‘\r’ (carriage return) are also used to improve readability.

CODE ADDRESS	OBFUSCATED ADDRESS	DEOBFUSCATED STRING
10001022	100220C0	"LocalFree"
10001071	100220CC	"GetOEMCP"
100010BB	100220D8	"GetCommandLineW"
10001105	100220EC	"GetCurrentProcess"
1000114F	10022100	"Sleep"
1000119E	10022108	"ExitProcess"
100011EA	10022118	"TerminateProcess"
1000123B	1002212C	"lstrcmpiW"
1000128D	10022138	"WaitForSingleObject"
100012DF	10022160	"SetEvent"
1000132E	1002216C	"GetLastError"
10001378	100221B0	"CommandLineToArgvW"
100013F5	10022150	"TlsSetValue"
10001761	100221C4	"SeDebugPrivilege"
100017A2	100221E8	"SeTcbPrivilege"
10001A97	1002217C	"SetServiceStatus"
10001B6A	**10022208**	**"SMI"**[51]
10001BD6	**10022214**	**"SMU"**
10001C47	**10022220**	**"SMRAC"**
10001C8A	**10022230**	**"SMRACU"**
10001DA0	10022190	"RegisterServiceCtrlHandlerExW"
10003AD9	10022240	"GetProcessHeap"
10003B23	1002225C	"HeapFree"
10003B8F	10022250	"HeapAlloc"
10003C64	10022268	"FreeLibrary"
10003CCD	**10022278**	**"ntdll.dll**[52]**"**
10003D03	**10022284**	**"kernel32.dll"**
10003D46	**10022294**	**"user32.dll"**
10003D8A	**100222A0**	**"advapi32.dll"**
10003DC9	**100222B0**	**"gdi32.dll"**
10003E09	**100222BC**	**"ws2_32.dll"**
10003E4C	**100222C8**	**"shell32.dll"**
10003E90	**100222D8**	**"shlwapi.dll"**
10003ED2	**100222E8**	**"psapi.dll"**
10003F12	**100222F4**	**"mpr.dll"**
10003F52	**10022300**	**"wtsapi32.dll"**
10003F88	**10022310**	**"version.dll"**
10003FC8	**10022320**	**"msvcrt.dll"**
10004008	**1002232C**	**"wininet.dll"**
10004048	**1002233C**	**"sfc.dll"**
10004089	**10022348**	**"odbc32.dll"**
100040C8	**10022354**	**"ole32.dll"**
10004101	**10022360**	**"iphlpapi.dll"**
10004151	10022370	"wsprintfA"
10004192	1002237C	"wsprintfW"
100047B7	10022388	"lstrlenA"
10004806	10022394	"lstrlenW"
10004855	100223A0	"MultiByteToWideChar"
100048B2	100223B8	"WideCharToMultiByte"
10004913	100223D0	"memcpy"
10004969	100223D8	"memset"
10004FC9	100223E0	"InitializeCriticalSection"
10005035	100223FC	"DeleteCriticalSection"
100050C5	10022414	"SetErrorMode"
10005109	10022424	"SeDebugPrivilege"
10005137	10022448	"SeTcpPrivilege"
100054DE	1002285C	"EnumServicesStatusW"

[51] SMI, SMU, SMRAC, SMRACU are the operating modes of ‘nateon.exe’. (Hauri - Response Team, 2011)

[52] The strings with suffix ‘.dll’ identify modules loaded dynamically by the malware.

Code Address	Obfuscated Address	Deobfuscated String
100056C8	100228A4	"QueryServiceConfig2W"
10005854	10022C34	"CompanyName"
1000589F	10022C50	"*"
100058DC	10022C58	"FileDescription"
10005927	10022C00	"*"
1000596E	10022C7C	"FileVersion"
100059B9	10022C98	"*"
100059F5	10022CA0	"ProductName"
10005A40	10022774	"*"
10005A8C	10022CBC	"ProductVersion"
10005AD7	10022CDC	"*"
10006021	10022468	"CloseHandle"
10006070	1002249C	"GetDiskFreeSpaceExW"
100060C8	100224B4	"GetVolumeInformationW"
1000612A	100224CC	"CreateDirectoryW"
1000617B	100224E0	"CreateFileW"
100061DB	100224F0	"GetFileSize"
1000622D	10022500	"GetFileTime"
10006285	10022510	"WriteFile"
100062E0	1002251C	"ReadFile"
1000633B	10022528	"SetEndOfFile"
1000638A	10022538	"SetFileTime"
100063E2	10022548	"SetFilePointer"
1000643A	10022558	"FindFirstFileW"
1000648C	10022568	"FindNextFileW"
100064DE	10022578	"FindClose"
1000652D	10022584	"FlushFileBuffers"
1000657C	10022598	"lstrcpyW"
100065D0	100225A4	"CreateProcessW"
10006631	100225C8	"memcmp"
10006766	10022478	"QueryDosDeviceW"
100067B9	100225D0	"\Device\Floppy<\x00><\uA4BC><\u5CD1>"
100067D3	100225D0	"\Device\Floppy<\x00><\uA4BC><\u5CD1>"
10006862	1002248C	"GetDriveTypeW"
10006941	100225F0	"%s"
10006990	100225F8	"%s"
10006AC7	10022600	"*.*"
100076E4	100225B4	"SHFileOperationW"
10007ACC	1002263C	"WNetCloseEnum"
10007CD5	10022618	"WNetOpenEnumW"
10007DE6	10022628	"WNetEnumResourceW"
10007F65	10022650	"%s"
10007FB7	10022658	"%s"
10007FFC	10022660	"%s"
1000804F	10022668	"%s"
100081E5	10022670	"GetVersionExW"
1000825D	10022718	"SetTcpEntry"
100084B0	10022774	"*"
10008503	1002277C	"*"
10008544	10022764	"System"
1000856D	10022754	"System"
10008596	10022728	"System Idle Process"
1000875B	100226F8	"GetTcpTable"
1000884E	10022680	"AllocateAndGetTcpExTableFromStack"
100088F8	100226C8	"GetExtendedTcpTable"
10008B17	100227D0	"*"
10008B5F	100227D8	"*"
10008B99	100227C0	"System"
10008BC2	100227B0	"System"
10008BEB	10022784	"System Idle Process"
10008DC4	10022708	"GetUdpTable"
10008E9C	100226A4	"AllocateAndGetUdpExTableFromStack"
10008F46	100226E0	"GetExtendedUdpTable"
10008FDE	100227E0	"WaitForMultipleObjects"
100093DD	100227F8	"GetIconInfo"
1000942F	10022808	"DestroyIcon"
1000947E	10022818	"OpenProcess"
100094D2	10022828	"OpenSCManagerW"
10009525	10022838	"OpenServiceW"
1000957A	10022848	"CloseServiceHandle"
100095C9	10022874	"QueryServiceConfigW"
10009623	1002288C	"ChangeServiceConfigW"
10009683	100228BC	"DeleteService"
100096D2	100228CC	"StartServiceW"
10009725	100228DC	"ControlService"
10009779	100228EC	"CreateDCW"
100097CE	100228F8	"GetDIBits"
1000982C	10022904	"DeleteDC"
1000987B	10022910	"DeleteObject"
100098CA	10022920	"ExtractIconExW"
10009923	10022930	"EnumProcesses"
10009978	10022940	"EnumProcessModules"
100099D0	10022954	"GetModuleFileNameExW"
10009A28	10022984	"SfcIsFileProtected"
10009D14	10022A24	"*"
10009D42	10022A2C	"*"
10009D7E	100229F8	"NT AUTHORITY"
10009DAD	10022A14	"SYSTEM"
10009DD6	100229CC	"NT AUTHORITY"
10009E05	100229E8	"SYSTEM"
10009E39	100229A0	"NT AUTHORITY"
10009E6B	100229BC	"SYSTEM"
10009ECA	10022A80	"*"
10009F13	10022A70	"System"

Code Address	Obfuscated Address	Deobfuscated String
10009F42	10022A60	"System"
10009F6E	10022A34	"System Idle Process"
10009F9A	10022A88	"CompanyName"
10009FDB	10022AA4	"*"
1000A020	10022AAC	"FileDescription"
1000A064	10022A24	"*"
1000A0A9	10022AD0	"FileVersion"
1000A0ED	10022AEC	"*"
1000A131	10022AF4	"ProductName"
1000A175	10022998	"*"
1000A1AF	10022B10	"ProductVersion"
1000A1F3	10022B30	"*"
1000A730	1002296C	"GetModuleInformation"
1000A7CC	10022B38	"*"
1000A805	10022B40	"\??\<\x00><\uFC04><\uF06C>"
1000A859	10022B4C	"\SystemRoot\<\x00><\u7C84><\u98E4>"
1000A8AE	10022B68	"\<\x00><\uFFFD>"
1000A919	10022B70	"CompanyName"
1000A95B	10022B8C	"*"
1000A999	10022B94	"FileDescription"
1000A9D8	10022BB8	"*"
1000AA13	10022BC0	"FileVersion"
1000AA52	10022BDC	"*"
1000AA8E	10022BE4	"ProductName"
1000AAD0	10022C00	"*"
1000AB0E	10022C08	"ProductVersion"
1000AB50	10022C28	"*"
1000B445	10022CE4	"DISPLAY"
1000B6A3	10022CF8	"SYSTEM\CurrentControlSet\Services\<\x00><\u90A0>ÜÐ"
1000B6DB	10022D40	"\Parameters<\x00><\u3858>"
1000B70E	10022D5C	"ServiceDll"
1000B77F	10022D74	"RegOpenKeyExW"
1000B7DD	10022D84	"RegCreateKeyExW"
1000B83D	10022D98	"RegQueryValueExW"
1000B899	10022DAC	"RegSetValueExW"
1000B8F8	10022DBC	"RegEnumKeyExW"
1000B953	10022DCC	"RegCloseKey"
1000B9A2	10022DDC	"SHCopyKeyW"
1000B9F9	10022E08	"SHDeleteKeyW"
1000BA4B	10022E18	"SHDeleteValueW"
1000BAA0	10022E28	"SHGetValueW"
1000BE37	10022DE8	"SHEnumKeyExW"
1000C492	10022DF8	"SHEnumValueW"
1000CAFB	10022E38	"VirtualAlloc"
1000CB53	10022E48	"VirtualFree"
1000CBA9	10022E58	"GetProcessWindowStation"
1000CBF3	10022E88	"SetProcessWindowStation"
1000CC42	10022EA4	"CloseWindowStation"
1000CC91	10022EB8	"OpenInputDesktop"
1000CCE4	10022ECC	"SetThreadDesktop"
1000CD33	10022EE0	"GetThreadDesktop"
1000CD82	10022EF4	"CloseDesktop"
1000CDD1	10022F04	"SetCursorPos"
1000CE23	10022F44	"GetCurrentThreadId"
1000CE6D	10022F58	"CreateThread"
1000CEC8	10022F68	"CreateCompatibleDC"
1000CF17	10022F7C	"CreateDIBSection"
1000CF72	10022F90	"SetDIBColorTable"
1000CFC9	10022FA4	"GdiFlush"
1000D013	10022FB0	"GetDeviceCaps"
1000D067	10022FC0	"BitBlt"
1000D0C9	10022FC8	"SelectObject"
1000D136	10022FD8	"DISPLAY"
1000DB81	10022FEC	"DISPLAY"
1000DE8A	10023000	"DISPLAY"
1000E3BE	10023014	"DISPLAY"
1000E9AB	10022F34	"PostMessageA"
1000EA13	10022F24	"keybd_event"
1000EA8B	10022F14	"mouse_event"
1000EB1C	10023028	"WinSta0"
1000EB3F	10022E74	"OpenWindowStationW"
1000EC3C	1002303C	"GetTickCount"
1000EC86	1002304C	"ConnectNamedPipe"
1000ECD8	10023060	"CreateNamedPipeW"
1000ED3F	10023074	"GetOverlappedResult"
1000ED96	1002308C	"CreateEventW"
1000F0CF	1002309C	"\\.\pipe\a%d<\x00><\u3CC4><\u3C18><\u9C08><\u3C8A>"
1000F2B1	100230B8	"\\.\pipe\b%d<\x00><\u7080><\u0C17><\u4C49><\uEC10>"
1000F38F	100230D4	"CMD.EXE"
1000FC7B	**100230E8**	**"SQLAllocHandle"**[53]
1000FCD0	**100230F8**	**"SQLSetEnvAttr"**
1000FD2A	**10023108**	**"SQLDriverConnectW"**
1000FD88	**1002311C**	**"SQLDisconnect"**
1000FDD7	**1002312C**	**"SQLFreeHandle"**
1000FE29	**1002313C**	**"SQLExecDirectW"**
1000FE7D	**1002315C**	**"SQLNumResultCols"**
1000FECF	**1002319C**	**"SQLMoreResults"**
10010339	**10023170**	**"SQLColAttributeW"**
100104B5	**10023184**	**"SQLFetch"**
1001052B	**10023190**	**"SQLGetData"**
1001057D	100231AC	"NULL"
10010627	**1002314C**	**"SQLGetDiagRecW"**

[53] The imported functions with an 'SQL' prefix were presumably used to access the SK Communications databases.

Code Address	Obfuscated Address	Deobfuscated String
10010739	100231DC	"ExitWindowsEx"
1001078A	100231EC	"InitiateSystemShutdownA"
10010808	100231C8	"LockWorkStation"
100108CC	10023208	"SeShutdownPrivilege"
100109C8	10023234	"SeShutdownPrivilege"
10010ACC	10023260	"SeShutdownPrivilege"
10010D37	100231B8	"MessageBoxW"
10010D95	100232F0	"GetConsoleMode"
10010DE7	10023318	"SetConsoleCtrlHandler"
10010E3B	1002337C	"SetConsoleScreenBufferSize"
10010EC2	10023330	"WriteConsoleInputW"
10010F47	100232CC	"GetConsoleCP"
10010FC1	100232DC	"GetConsoleOutputCP"
10011044	10023300	"GetConsoleDisplayMode"
10011096	100233AC	"GetConsoleCursorInfo"
1001110F	10023360	"GetConsoleScreenBufferInfo"
1001134D	10023398	"ReadConsoleOutputW"
10011617	100233D4	"CMD"
10011643	100233E0	" "
1001166F	100233E8	"/Q"
100116A3	100232A8	"AllocConsole"
100116F3	100232B8	"GetConsoleWindow"
10011738	1002328C	"ShowWindow"
100117A2	10023298	"GetStdHandle"
10011AE2	100233C4	"FreeConsole"
10011CAA	100233F0	"CONIN$"
10011D3A	10023344	"GenerateConsoleCtrlEvent"
10011E6D	10023400	"CONIN$"
10011EAD	10023410	"CONOUT$"
10011F88	10023424	"CreateWindowExW"
10011FE7	10023438	"SetWindowLongW"
1001203D	10023448	"DestroyWindow"
1001208C	10023458	"TranslateMessage"
100120DB	1002347C	"SetTimer"
10012136	10023488	"KillTimer"
10012188	100234A4	"DispatchMessageW"
100121D7	100234F8	"WTSUnRegisterSessionNotification"
100122CB	10023494	"PeekMessageW"
10012379	1002351C	"static"
1001255F	100234D8	"WTSRegisterSessionNotification"
10012687	100234B8	"MsgWaitForMultipleObjectsEx"
10012779	1002346C	"DefWindowProcW"
10012C0D	1002356C	"QueryPerformanceCounter"
10012C5C	1002359C	"GetFileAttributesW"
10012CAB	100235B0	"ExpandEnvironmentStringsW"
10012D00	100235CC	"GetModuleFileNameW"
10012D55	100235E0	"OpenProcessToken"
10012DAA	100235F4	"GetLengthSid"
10012DF9	10023604	"GetTokenInformation"
10012E54	10023630	"LookupPrivilegeValueW"
10012EA8	10023648	"AdjustTokenPrivileges"
10012F02	100236B4	"GetFileVersionInfoW"
10012F59	100236CC	"VerQueryValueW"
100130F1	1002353C	"GetWindowsDirectoryW"
10013158	10023554	"GetSystemDirectoryW"
100132AD	10023588	"GetComputerNameW"
1001337D	10023660	"GetUserNameW"
10013445	10023748	"CLSID"
10013465	**10023758**	**"SOFTWARE\CLASSES\SAFEGUI<\x00><\u40F0><\u380B>"**[54]
100134D4	1002378C	"CLSID"
100134EA	**10023758**	**"SOFTWARE\CLASSES\SAFEGUI<\x00><\u40F0><\u380B>"**
1001357C	1002352C	"GetSystemTime"
100136DC	100237A0	"%2.2X%2.2X%2.2X%2.2X%2.2X%2.2X%2.2X%2.2X"
10013749	100237F4	"%ALLUSERSPROFILE%"
100137C6	10023820	"\Documents and Settings\All Users<\x00><\uC030><\u0848>"
10013807	10023868	"\Documents and Settings\All Users<\x00><\u78D8><\u6090>"
1001384C	100238B0	"\Documents and Settings\All Users<\x00><\u3818><\u20D0>"
1001389A	100238F8	"\ProgramData<\x00><\uE8A8>"
100138D8	10023914	"\ProgramData<\x00><\uFFFD>"
10013907	10023930	"\<\x00><\uB898>"
10013B54	10023938	"*.*<\x00><\u140C>"
10013E1F	10023944	".EXE"
10013EFB	10023950	".EXE"
1001404B	1002395C	"\??\<\x00><\u742C><\uCC38>"
1001409E	10023968	"\SystemRoot\<\x00><\u0808><\u5834>"
100140F1	10023984	"\<\x00><\u18B8>"
10014219	1002361C	"LookupAccountSidW"
100143AE	10023670	"WTSEnumerateProcessesW"
10014461	10023688	"WTSFreeMemory"
100144FB	10023698	"GetFileVersionInfoSizeW"
1001459E	1002398C	"\VarFileInfo\Translation<\x00><\uEC54><\u2C48>"
10014605	100239C0	"\StringFileInfo\%4.4X%4.4X\%s<\x00><\uF8D8><\uE090><\u2379>"
10014992	10023A00	"IsWow64Process"

[54] The unusual hardcoded registry key 'SOFTWARE\CLASSES\SAFEGUI' can be used to link 'nateon.exe' with the malware that has the MD5 hash 6C6A DBD0 8727 6AE8 9F82 6258 2798 B708 and calls back to the domain 'expre.dyndns.tv' on TCP port 443. It may also be used as a signature to identify other similar malware. (GFI SandBox, 2011)

Code Address	Obfuscated Address	Deobfuscated String
100149F5	10023A10	"GetCurrentProcessId"
10014A3F	10023A28	"ProcessIdToSessionId"
10014A91	10023A40	"DuplicateTokenEx"
10014AEE	10023A54	"SetTokenInformation"
10014B46	10023A98	"CreateProcessAsUserW"
100151CE	10023AB0	".DLL"
10015202	10023ABC	"RUNDLL32.EXE "
1001522E	10023ADC	""<\x00><\u6010>"
10015268	10023AE4	"\<\x00><\u3080>"
100152A0	10023AEC	"" <\x00><\u6868>"
100152CC	10023AF4	"RqSkce"
100152F8	10023B04	" "
10015324	10022220	"SMRAC"
100153FC	**10023B0C**	**"UserEnv.dll"**
1001542A	10023B1C	"CreateEnvironmentBlock"
10015456	10023B34	"DestroyEnvironmentBlock"
100155C1	10023B50	".DLL"
1001561B	10023B5C	"RUNDLL32.EXE "
10015656	10023B7C	""<\x00><\u843C>"
1001569E	10023B84	"\<\x00><\u68A8>"
100156EF	10023B8C	"" <\x00><\uCCF4>"
10015722	10023AF4	"RqSkce"
1001575D	10023B04	" "
10015790	10022230	"SMRACU"
100157E1	10023A6C	"ImpersonateLoggedOnUser"
1001586B	10023A88	"RevertToSelf"
10015943	10023B94	"WTSGetActiveConsoleSessionId"
10015C5E	10023BB4	"NT AUTHORITY"
10015D15	10023BF0	"MoveFileExW"
10015D68	10023C00	"GetModuleHandleA"
100160D5	**10023C28**	**"%SystemRoot%\system32\svchost.exe -k LocalService<\x00><\uBC64><\uD4CC>"**[55]
10016108	10023C90	"SYSTEM\CurrentControlSet\Services<\x00><\u54AC><\u8C34>"
10016138	10023CD8	"\<\x00><\uC4FC>"
10016183	10023CE0	"\Parameters<\x00><\uA8A8>"
100161C2	10023CFC	"LocalService"
10016267	10023D18	"ServiceDll"
100162B6	10023AF4	"RqSkce"
100162C8	10023AF4	"RqSkce"
100162E3	10023D30	"ServiceMain"
10016389	10023D4C	"LocalService"
100163EF	10023D68	".DLL"
1001642B	10023D74	"\<\x00><\u344C>"
1001649E	10023D7C	"RUNDLL32.EXE "
100164D0	10023D9C	""<\x00><\u8070>"
10016519	10023DA4	"" <\x00><\u74AC>"
1001654C	10023AF4	"RqSkce"
10016582	10023DAC	" "
100165BE	10022208	"SMI"
100165FD	10023DB4	" "
1001663B	10023DBC	""<\x00><\u14EC>"
10016691	10023DC4	""<\x00><\u28E8>"
1001689E	10023BE0	"DeleteFileW"
100169F3	10023C14	"GetModuleFileNameA"
10016A4A	10023BD0	"CreateFileA"
10016DAA	10023DEC	"QueryServiceStatusEx"
10016E03	10023E04	"ChangeServiceConfig2W"
10016E59	10023E1C	"CreateServiceW"
1001779C	10023E30	"SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost<\x00><\uA8E8><\uC40C><\uFFFD><\u9050>"
1001791E	10023E9C	""
10017956	10023E30	"SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost<\x00><\uA8E8><\uC40C><\uFFFD><\u9050>"
10017A37	10023E30	"SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost<\x00><\uA8E8><\uC40C><\uFFFD><\u9050>"
10017BE1	10023EA0	""
10017C10	10023E30	"SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost<\x00><\uA8E8><\uC40C><\uFFFD><\u9050>"
10017C5F	10023EA4	"VirtualAllocEx"
10017CBC	10023EB4	"VirtualFreeEx"
10017D15	10023EC4	"WriteProcessMemory"
10017D74	10023EEC	"GetWindowThreadProcessId"
10017DC6	10023F18	"GetExitCodeThread"
10017E18	10023F48	"EqualSid"
10017E6A	10023F54	"FreeSid"
10017EB9	10023F60	"ShellExecuteExW"
10017F08	10023F74	"SHCreateItemFromParsingName"
10017F61	10023FA4	"CoCreateInstance"
10018226	10023F2C	"AllocateAndInitializeSid"
100184E2	10023FC8	".DLL"
10018534	10023FD4	""<\x00><\u7CA4>"
1001856E	10023FDC	"\<\x00><\u9C04>"
100185A6	10023FE4	"" <\x00><\u1020>"
100185D2	10023AF4	"RqSkce"
100185FE	10023FEC	" "
1001862A	10022208	"SMI"
100186F4	**1002401C**	**"\SYSPREP<\x00><\uF8D8>"**
10018720	**10024030**	**"\SYSPREP.EXE<\x00><\u18B8>"**

[55] The 'nateon.exe' dropper configures 'winsvcfs.dll' to run inside the trusted operating system process 'svchost.exe'.

Code Address	Obfuscated Address	Deobfuscated String
1001881A	10024058	"LoadLibraryW"
10018836	**10024068**	**"kernel32.dll"**
10018879	10024078	"FreeLibrary"
10018890	**10024068**	**"kernel32.dll"**
10018B30	10022B68	"\<\x00><\uFFFD>"
10018B71	10024088	"sysprep"
10018BE4	10023F94	"CoInitializeEx"
10018C88	**1002409C**	**"CRYPTBASE.DLL"**
10018D00	100240BC	"\<\x00><\u5C44>"
10018D3A	100240C4	"sysprep"
10018D7D	100240D8	"\<\x00><\u0888>"
10018DBB	**100240E0**	**"CRYPTBASE.DLL"**
10018E1B	10024100	"\<\x00><\u1020>"
10018E46	100240C4	"sysprep"
10018E75	10024108	"\<\x00><\u8070>"
10018EA7	10024110	"sysprep.exe"
10018FB8	10023FB8	"CoUninitialize"
1001903E	**1002412C**	**"CRYPTBASE.DLL"**
100190B1	1002414C	".DLL"
10019112	10024158	"RUNDLL32.EXE "
1001914B	10024178	""<\x00><\uF858>"
10019197	10024180	"\<\x00><\u6010>"
100191E0	10024188	"" <\x00><\uF42C>"
10019219	10023AF4	"RqSkce"
10019252	10024190	" "
1001928B	10022208	"SMI"
1001949A	10023ED8	"CreateRemoteThread"
10019534	10024198	"Shell_TrayWnd"
10019558	10023F08	"FindWindowA"
100195E4	100241C8	"GetCurrentThread"
1001962E	100241DC	"SetThreadPriority"
100197F3	10024204	"GetSystemMetrics"
10019842	10024230	"gethostbyname"
10019891	10024240	"lstrcatW"
100198E3	1002424C	"ResumeThread"
10019939	1002425C	"QueueUserAPC"
1001A25C	100242C8	"\\.\PIPE\RUN_AS_CONSOLE_USER(%d)<\x00><\u0CB4><\u40E5><\u4033><\uC0C0>"
1001A419	**1002426C**	**"download.windowsupdate.com"**[56]
1001A66A	10024288	"\\.\PIPE\RUN_AS_CONSOLE(%d)<\x00><\u7000><\u78D8><\u6090><\u2828>"
1001A914	100241F0	"GlobalMemoryStatus"
1001AA61	100236DC	"~MHZ"
1001AA7F	100236E8	"HARDWARE\DESCRIPTION\SYSTEM\CENTRALPROCESSOR\0<\x00><\u70C0><\u28FB><\u38E4><\u680B>"
1001AB05	10024218	"GetSystemDefaultLCID"
1001AB81	1002430C	"%s"
1001ABC1	10022658	"%s"
1001AC02	10024314	""
1001AC23	10024318	"%s"
1001AC6B	10024320	"%s"
1001ACA4	10022658	"%s"
1001ACE1	10024328	""
1001ACFC	1002432C	"%s"
1001B0D7	10024334	".DLL"
1001B11A	10024340	"RUNDLL32.EXE "
1001B15A	10024360	""<\x00><\u5878>"
1001B1B4	10023FDC	"\<\x00><\u9C04>"
1001B1F4	10024368	"" <\x00><\u9CE4>"
1001B22C	10023AF4	"RqSkce"
1001B266	10024370	" "
1001B29B	10022214	"SMU"
1001B54A	10024378	"RtlNtStatusToDosError"
1001B599	100243B0	"RtlDecompressBuffer"
1001B5F8	100243C8	"RtlCompressBuffer"
1001B677	10024390	"RtlGetCompressionWorkSpaceSize"
1001BD1B	10024288	"\\.\PIPE\RUN_AS_CONSOLE(%d)<\x00><\u7000><\u78D8><\u6090><\u2828>"
1001BEDB	100243DC	"TerminateThread"
1001BF2F	10024418	"SetUnhandledExceptionFilter"
1001BF7E	100243F0	"TlsAlloc"
1001C028	1002440C	"TlsFree"
1001C0CB	100243FC	"TlsGetValue"
1001C139	10024438	"ECount=%d,"
1001C180	10024450	"EAddr=0x%p,"
1001C1CC	1002446C	"ECode=0x%x,"
1001C214	10024488	"ESalF=%d"
1001C2D4	1002449C	"MessageBoxA"
1001C32C	100244AC	"lstrcpyA"
1001C380	100244B8	"InternetOpenA"
1001C3D4	100244C8	"InternetOpenUrlA"
1001C431	100244DC	"InternetReadFile"
1001C489	100244F0	"InternetCloseHandle"
1001C510	**10024508**	**"XXXXXXXX"**[57]
1001C5E3	**10024514**	**"DEMO"**
1001C618	**10024520**	**"TVT"**
1001C658	**10024528**	**"TVT DEMO"**
1001C6DA	**10024534**	**"192.168.0.200"**

[56] The hardcoded domain name 'download.windowsupdate.com' is used to detect internet connectivity. This domain name can be overridden in the malware's configuration.

[57] This set of hardcoded strings, 'XXXXXXXX', 'DEMO', 'TVT', 'TVT DEMO', and '192.168.0.200' are hardcoded values overridden by the malware's configuration.

Code Address	Obfuscated Address	Deobfuscated String
1001C717	**10024534**	**"192.168.0.200"**
1001C74F	10024548	""
1001C7BF	**1002454C**	**"CONFIG-DESTORY!"**[58]
1001CC41	10024560	"%2.2X"
1001CCB2	**10024570**	**"Software\SafeSvc<\x00><\uB4EC>"**[59]
1001CD54	10024594	"%2.2X"
1001CD98	100245A4	"Software\SafeSvc<\x00><\u40F0>"
1001CDE7	100245C8	"socket"
1001CE41	100245D0	"bind"
1001CE94	100245E0	"setsockopt"
1001CEEE	100245EC	"shutdown"
1001CF3F	100245F8	"closesocket"
1001CF95	10024608	"ioctlsocket"
1001CFEC	10024620	"htons"
1001D03B	10024634	"WSAGetLastError"
1001D085	10024648	"lstrcpynA"
1001D45C	100245D8	"recv"
1001D5C1	10024654	""
1001D67C	**10024658**	**"Proxy-Authorization: Basic "**
1001D6B5	**10024678**	**"GET "**
1001D6E8	**10024680**	**"POST "**
1001D71B	**10024688**	**"CONNECT "**
1001D775	**10024658**	**"Proxy-Authorization: Basic "**
1001D886	10024694	""
1001DA8F	10024618	"ntohs"
1001DB03	10024628	"inet_ntoa"
1001E16D	100246C8	"ResetEvent"
1001E1BE	100246D4	"InternetConnectA"
1001E21A	100246E8	"InternetWriteFile"
1001E272	10024710	"HttpSendRequestExA"
1001E2CA	10024724	"HttpEndRequestA"
1001E31F	10024748	"InternetSetOptionA"
1001E376	1002475C	"HttpAddRequestHeadersA"
1001E3CF	10024698	"EnterCriticalSection"
1001E420	100246B0	"LeaveCriticalSection"
1001EE91	**10024774**	**"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;SV1;"**[60]
1001EF9B	**100247B0**	**"/update?product=windows"**[61]
1001EFB6	**100247CC**	**"POST"**
1001EFDD	100246FC	"HttpOpenRequestA"
1001F113	10024560	"%2.2X"
1001F189	10024570	"Software\SafeSvc<\x00><\uB4EC>"
1001F278	100247D4	":"
1001F308	**100247D8**	**"Proxy-Authorization: Basic %s<\r><\n><\x00>öL"**
1001F39B	**100247FC**	**"X-Session"**[62]
1001F3BC	10024808	"%s: %d"
1001F41E	**10024810**	**"X-Status"**
1001F43F	1002481C	"%s: %d"
1001F49B	**10024824**	**"X-Size"**
1001F4B9	1002482C	"%s: %d"
1001F507	**10024834**	**"X-Sn"**
1001F525	1002483C	"%s: %d"
1001F776	10024844	""
1001F7BB	10024848	""
1001F7FC	**100247FC**	**"X-Session"**
1001F845	**10024810**	**"X-Status"**
1001F889	**10024824**	**"X-Size"**
1001F8CD	**10024834**	**"X-Sn"**
1001FC5C	1002484C	"%s"
1001FC90	10024738	"HttpQueryInfoA"
10020324	10024850	"connect"
10020378	1002486C	"getpeername"
100203CF	10024894	"WSAIoctl"
10020430	100248A0	"WSAGetOverlappedResult"
10020662	100248B8	"WSAStartup"
100206C5	100248C4	"WSACleanup"
10020A04	**100248D0**	**"CONNECT %s:%d HTTP/1.1<\r><\n><\x00>d$"**
10020A46	**100248EC**	**"Content-length: 0<\r><\n><\x00>tl"**
10020A7A	**10024904**	**"Content-Type: text/html<\r><\n><\x00>|d"**
10020AAE	**10024920**	**"Proxy-Connection: Keep-Alive<\r><\n><\x00><\u2584><\u20A7>"**
10020B10	10024940	":"
10020B63	**10024944**	**"Proxy-Authorization: Basic %s<\r><\n><\x00><\u255D>"**
10020C3E	**10024968**	**"HTTP/1.0 200 "**
10020C79	**10024978**	**"HTTP/1.1 200 "**
1002124B	1002485C	"getsockname"
100212C1	1002487C	"WSASend"
1002134E	10024888	"WSARecv"
10021438	10024998	"static"
100214B6	10024988	"GetMessageW"

[58] The string 'CONFIG-DESTORY!' is displayed in a message box when 'nateon.exe' detects corruption in its configuration. It can be used as a signature to identify similar malware.

[59] The unusual hardcoded registry key 'Software\SafeSvc' can be used as a signature to identify similar malware.

[60] This is the user-agent included in HTTP requests made by the malware to its configured command and control infrastructure. This malformed user-agent string can be used as a signature to detect malicious network traffic.

[61] This is the path included in HTTP requests made by 'nateon.exe' to its configured command and control infrastructure. This string can be used as a signature to detect malicious network activity.

[62] The HTTP headers 'X-Session', 'X-Status', 'X-Size', and 'X-Sn' can be used to develop stronger signatures for detection of network activity generated by the malware.

ANNEX B

SUMMARY OF MALWARE KNOWN TO CREATE THE UNIQUELY NAMED DIRECTORY: '03A075FB70D5D675F9DC26FC'

MD5 HASH	FILE SIZE (BYTES)	DATE(S) ANALYSED	FILES CREATED	NETWORK CONNECTIVITY
16A3 1AA8 E7DD F66A 3155 1840 573B 6575	155648	13 July 2011 (ThreatExpert, 2011)	$$$$$$$$mtx.bat winscard2.exe	TCP port 1058 opened for inbound connections
ABA9 BAEA 7082 5E6A DF07 2358 7F27 3DC4	3514598	29 July 2011 (ThreatExpert, 2011)	zhenxiang.exe winscard.exe	TCP ports 1052 and 1053 opened for inbound connections
BCE1 069D D099 F151 70C5 FD05 BAE9 21B5	133632	29 May 2011 (GFI SandBox, 2011) 03 August 2011 (ThreatExpert, 2011)	106140_d.bat tcmoniter.exe	pc.nprotects.org on TCP port 80
E8EE 9373 EE6C 8360 42E8 F48D 8DE2 DDA9	unknown	08 February 2011 (GFI Software, 2011)	$$$$$$$$fbl.bat tcomoniter.exe	pc.nprotects.org on TCP port 80
FDF2 C5C2 B187 4EFE 7FD3 3509 2DF2 D3BC	unknown	15 July 2011 (GFI SandBox, 2011)	40984_d.bat wincard0.dll uxtheme.dll	bbs.ezxsoft.com on TCP port 80

COPYRIGHT NOTICE

Command Five Pty Ltd
ABN: 49 149 576 670

http://www.commandfive.com
info@commandfive.com