

[Content menu](#)[Subscribe](#)

ShadowPad in corporate networks

APT REPORTS

15 AUG 2017

⌚ 5 minute read



// AUTHORS

Expert

GREAT

Popular server management software hit in supply chain attack

[ShadowPad, part 2: Technical Details \(PDF\)](#)

In July 2017, during an investigation, suspicious DNS requests were identified in a partner's network. The partner, which is a financial institution, discovered the requests originating on systems involved in the processing of financial transactions.

Further investigation showed that the source of the suspicious DNS queries was a software package produced by [NetSarang](#). Founded in 1997, NetSarang Computer, Inc.

GREAT WEBINARS

13 MAY 2021, 1:00PM

GReAT Ideas. Balalaika Edition

[BORIS LARIN](#), [DENIS LEGEZO](#)

26 FEB 2021, 12:00PM

GReAT Ideas. Green Tea Edition

[JOHN HULTQUIST](#), [BRIAN BARTHOLOMEW](#), [SUGURU ISHIMARU](#),
[VITALY KAMLUK](#), [SEONGSU PARK](#), [YUSUKE NIWA](#),
[MOTOHIKO SATO](#)

17 JUN 2020, 1:00PM

GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots

[MARCO PREUSS](#), [DENIS LEGEZO](#), [COSTIN RAIU](#),
[KURT BAUMGARTNER](#), [DAN DEMETER](#), [YAROSLAV SHMELEV](#)

26 AUG 2020, 2:00PM

GReAT Ideas. Powered by SAS: threat actors advance on new fronts

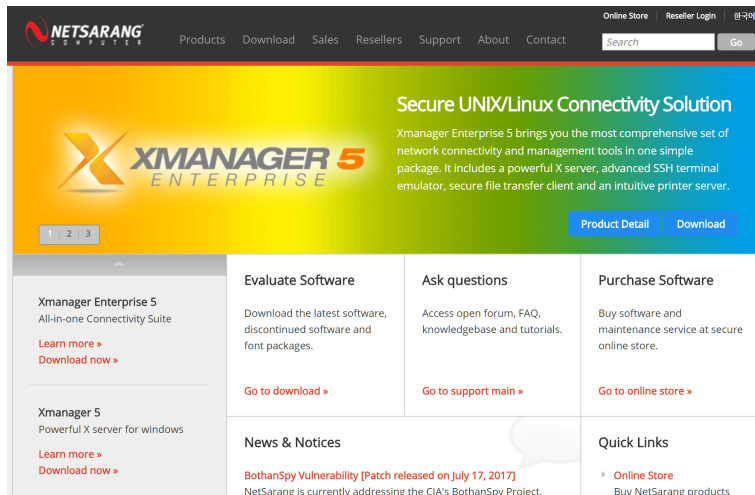
[IVAN KWIATKOWSKI](#), [MAHER YAMOUT](#), [NOUSHIN SHABAB](#),
[PIERRE DELCHER](#), [FÉLIX AIME](#), [GIAMPAOLO DEDOLA](#),
[SANTIAGO PONTIROLI](#)

22 JUL 2020, 2:00PM

GReAT Ideas. Powered by SAS: threat hunting and new techniques

[DMITRY BESTUZHEV](#), [COSTIN RAIU](#), [PIERRE DELCHER](#),
[BRIAN BARTHOLOMEW](#), [BORIS LARIN](#), [ARIEL JUNGHEIT](#),
[FABIO ASSOLINI](#)

develops, markets and supports secure connectivity solutions and specializes in the development of server management tools for large corporate networks. The company maintains headquarters in the United States and South Korea.



NetSarang website

Our analysis showed that recent versions of software produced and distributed by NetSarang had been surreptitiously modified to include an encrypted payload that could be remotely activated by a knowledgeable attacker.

The backdoor was embedded into one of the code libraries used by the software (nssock2.dll):

Backdoored dll in a list of loaded modules of Xshell5 software

Disposition of the NSSOCK2.DLL binary with embedded malicious code

The attackers hid their malicious intent in several layers of encrypted code. The tiered architecture prevents the actual business logics of the backdoor from being activated until a special packet is received from the first tier command and control (C&C) server ("activation C&C server"). Until then, it only transfers basic information, including the computer, domain and user names, every 8 hours.

Activation of the payload would be triggered via a specially crafted DNS TXT record for a specific domain. The domain name is generated based on the current month and year values, e.g. for August 2017 the domain name used would be "nylaloghyhirgh.com".

FROM THE SAME AUTHORS

DNS queries to C&C from backdoored nssock2.dll

***Only when triggered by the first layer of C&C servers
does the backdoor activate its second stage***

The module performs a quick exchange with the controlling DNS server and provides basic target information (domain and user name, system date, network configuration) to the server. The C&C DNS server in return sends back the decryption key for the next stage of the code, effectively activating the backdoor. The data exchanged between the module and the C&C is encrypted with a proprietary algorithm and then encoded as readable latin characters. Each packet also contains an encrypted "magic" DWORD value "52 4F 4F 44" ('DOOR' if read as a little-endian value).

Our analysis indicates the embedded code acts as a modular backdoor platform. It can download and execute arbitrary code provided from the C&C server, as well as maintain a virtual file system (VFS) inside the registry. The VFS, and any additional files created by the code, are encrypted and stored in a location unique to each victim. The remote access capability includes a domain generation algorithm (DGA) for C&C servers which changes every month. The attackers behind this malware have already registered the domains covering July to December 2017, which indirectly confirms alleged start date of the attack as around mid July 2017.

Android malware, Android malware and more Android malware

Coyote: A multi-stage banking Trojan abusing the Squirrel installer

FakeSG campaign, Akira ransomware and AMOS macOS stealer

Advanced threat predictions for 2024

Stealer for PIX payment system, new Lumar stealer and Rhysida ransomware

Currently, we can confirm activated payload in a company in Hong Kong. Given that the NetSarang programs are used in hundreds of critical networks around the world, on servers and workstations belonging to system administrators, it is **strongly** recommended that companies take immediate action to identify and contain the compromised software.

Kaspersky Lab products detect and protect against the backdoored files as "Backdoor.Win32.ShadowPad.a".

We informed NetSarang of the compromise and they immediately responded by pulling down the compromised software suite and replacing it with a previous clean version. The company has also published a message (https://www.netsarang.com/news/security_exploit_in_july_18_2017_build.html) acknowledging our findings and warning their customers.

ShadowPad is an example of the dangers posed by a successful supply-chain attack. Given the opportunities for covert data collection, attackers are likely to pursue this type of attack again and again with other widely used software components. Luckily, NetSarang was fast to react to our notification and released a clean software update, most likely preventing hundreds of data-stealing attacks against their clients. This case is an example of the value of threat research as a means to secure the wider internet ecosystem. No single entity is in a position to defend all of the links in an institution's software and hardware supply-chain. With successful and open cooperation, we can help weed out the attackers in our midst and protect the internet for all users, not just our own.

For more information please contact:

intelreports@kaspersky.com

Frequently Asked Questions

What does the code do if activated?

If the backdoor were activated, the attacker would be able to upload files, create processes, and store information in a VFS contained within the victim's registry. The VFS and any additional files created by the code are encrypted and stored in locations unique to each victim.

Which software packages were affected?

We have confirmed the presence of the malicious file (nssock2.dll) in the following packages previously available on the NetSarang site:

Xmanager Enterprise 5 Build 1232
Xme5.exe, Jul 17 2017, 55.08 MB
MD5: 0009f4b9972660eeb23ff3a9dccd8d86
SHA1: 12180ff028c1c38d99e8375dd6d01f47f6711b97

Xmanager 5 Build 1045
Xmgr5.exe, Jul 17 2017, 46.2 MB
MD5: b69ab19614ef15aa75baf26c869c9cdd
SHA1:
35c9dae68c129ebb7e7f65511b3a804ddbe4cf1d

Xshell 5 Build 1322
Xshell5.exe, Jul 17 2017, 31.58 MB
MD5: b2c302537ce8fbbcff0d45968cc0a826
SHA1:
7cf07efe04fe0012ed8beaa2dec5420a9b5561d6

Xftp 5 Build 1218
Xftp5.exe, Jul 17 2017, 30.7 MB
MD5: 78321ad1deefce193c8172ec982ddad1
SHA1:
08a67be4a4c5629ac3d12f0fdd1efc20aa4bdb2b

Xlpd 5 Build 1220
Xlpd5.exe, Jul 17 2017, 30.22 MB
MD5: 28228f337fdb3ab34316a7132123c49
SHA1:
3d69fdd4e29ad65799be33ae812fe278b2b2dabe

Subscribe to our weekly e-mails

The hottest research right in your inbox

☐

I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

Subscribe

Is NetSarang aware of this situation?

Yes, we contacted the vendor and received a swift response. Shortly after notification by Kaspersky Lab all malicious files were removed from NetSarang website.

How did you find the software was backdoored?

During an investigation, suspicious DNS requests were identified on a partner's network. The partner, which is a financial institution, detected these requests on systems related to the processing of financial transactions. Our analysis showed that the source of these suspicious requests was a software package produced by NetSarang.

When did the malicious code first appear in the software?

A fragment of code was added in nssock2.dll (MD5: 97363d50a279492fda14cbab53429e75), compiled Thu Jul 13 01:23:01 2017. The file is signed with a legitimate NetSarang certificate (Serial number: 53 0C E1 4C 81 F3 62 10 A1 68 2A FF 17 9E 25 80). This code is not present in the nssock2.dll from March (MD5: ef0af7231360967c08efbdd2a94f9808) included with the NetSarang installation kits from April.

How do I detect if code is present on a system?

All Kaspersky Labs products detect and cure this threat as Backdoor.Win32.Shadowpad.a. If for some reason you can't use an antimalware solution you can check if there were DNS requests from your organization to these domains:

ribotqtonut[.]com

nylalobghyhirgh[.]com

jkvmdmjyfcvkf[.]com

bafyvoruzgjitwr[.]com

xmponmzmxkxkh[.]com

tczafklirk[.]com

notped[.]com

dnsgoogle[.]com

operatingbox[.]com

paniesx[.]com

techniciantext[.]com

How do I clean any affected systems?

All Kaspersky Lab products successfully detect and disinfect the affected files as “Backdoor.Win32.Shadowpad.a” and actively protect against the threat.

If you do not have a Kaspersky product installed, then:

- 1 Update to the latest version of the NetSarang package.
- 2 Block DNS queries to the C2 domains listed in Appendix A.

What kind of companies/organizations/are targeted by the attackers?

Based on the vendor profile, the attackers could be after a broad set of companies who rely on NetSarang software, which includes banking and financial industry, software and media, energy and utilities, computers and electronics, insurance, industrial and construction, manufacturing, pharmaceuticals, retail, telecommunications, transportation and logistics and other industries.

Who is behind this attack?

Attribution is hard and the attackers were very careful to not leave obvious traces. However certain techniques were known to be used in another malware like PlugX and Winnti, which were allegedly developed by Chinese-speaking actors.

IN THE SAME CATEGORY

How did the attackers manage to get access to create trojanized updates. Does that mean that NetSarang was hacked?

An investigation is in progress, but since code was signed and added to all software packages it could point to the fact that attackers either modified source codes or patched software on the build servers.

Appendix A – Indicators of Compromise

At this time, we have confirmed the presence of the malicious “nssock2.dll” in the following packages downloaded from the NetSarang site:

Xmanager Enterprise 5 Build 1232
Xme5.exe, Jul 17 2017, 55.08 MB
MD5: 0009f4b9972660eeb23ff3a9dccc8d86
SHA1: 12180ff028c1c38d99e8375dd6d01f47f6711b97

Xmanager 5 Build 1045
Xmgr5.exe, Jul 17 2017, 46.2 MB
MD5: b69ab19614ef15aa75baf26c869c9cdd
SHA1:
35c9dae68c129ebb7e7f65511b3a804ddbe4cf1d

Xshell 5 Build 1322
Xshell5.exe, Jul 17 2017, 31.58 MB
MD5: b2c302537ce8fbbcff0d45968cc0a826
SHA1:
7cf07efe04fe0012ed8beaa2dec5420a9b5561d6

Xftp 5 Build 1218
Xftp5.exe, Jul 17 2017, 30.7 MB
MD5: 78321ad1deefce193c8172ec982ddad1
SHA1:
08a67be4a4c5629ac3d12f0fdd1efc20aa4bdb2b

Xlpd 5 Build 1220
Xlpd5.exe, Jul 17 2017, 30.22 MB
MD5: 28228f337fdb3ab34316a7132123c49
SHA1:

HrServ – Previously unknown web shell used in APT attack

Modern Asian APT groups' tactics, techniques and procedures (TTPs)

A cascade of compromise: unveiling Lazarus' new campaign

How to catch a wild triangle

StripedFly: Perennially flying under the radar

3d69fdd4e29ad65799be33ae812fe278b2b2dabe

Domains:

ribotqtonut[.]com
nylalobghyhirgh[.]com
jkvmdmjyfcvkf[.]com
bafyvoruzgjitwr[.]com
xmponmzmxkxkh[.]com
tczafklirk[.]com
notped[.]com
dnsgoogle[.]com
operatingbox[.]com
paniesx[.]com
techniciantext[.]com

DLL with the encrypted payload:

97363d50a279492fda14cbab53429e75

NetSarang packages which contain the DLL with the encrypted payload (same as above, just the list of MD5 sums):

0009f4b9972660eeb23ff3a9dccd8d86
b69ab19614ef15aa75baf26c869c9cdd
b2c302537ce8fbbcff0d45968cc0a826
78321ad1deefce193c8172ec982ddad1
28228f337fdbe3ab34316a7132123c49

File names:

nsock2.dll

APT

BACKDOOR

DNS

SUPPLY-CHAIN ATTACK

TARGETED ATTACKS

ShadowPad in corporate networks

Your email address will not be published. Required fields are marked *

Type your comment here

Name *

Email *

Comment

KEN HOLLIS

Posted on August 16, 2017. 8:11 pm

Since the domains have apparently disappeared can you give the IP address that they were last seen at?

Thanks

[Reply](#)

NIMA

Posted on August 16, 2017. 11:22 pm

this is only security exploit , not backdoor .

[Reply](#)

PATRICK HUNTER

Posted on September 8, 2017. 8:36 pm

There's malicious code actually inserted into the software which is then activated later; that is absolutely a backdoor. This isn't just some RCE exploit.

[Reply](#)



// LATEST POSTS

MALWARE REPORTS

Android malware, Android malware and more Android malware

GREAT

SOC, TI AND IR POSTS

A patched Windows attack surface is still exploitable

ELSAYED ELREFAEI,

ASHRAF REFAAT, KASPERSKY GERT

MALWARE DESCRIPTIONS

What's in your notepad? Infected text editors target Chinese users

SERGEY PUZAN

RESEARCH

Top 10 web application vulnerabilities in 2021–2023

OXANA ANDREEVA,

KASPERSKY SECURITY SERVICES

// LATEST WEBINARS

TECHNOLOGIES AND SERVICES

11 DEC 2023, 4:00PM 60 MIN

The Future of AI in cybersecurity: what to expect in 2024

VLADIMIR DASHCHENKO,

VICTOR SERGEEV,

VLADISLAV TUSHKANOV,

DENNIS KIPKER

THREAT INTELLIGENCE AND IR

30 NOV 2023, 4:00PM 70 MIN

Responding to a data breach: a step-by-step guide

ANNA PAVLOVSKAYA

CYBERTHREAT TALKS

14 NOV 2023, 4:00PM 60 MIN

2024 Advanced persistent threat predictions

IGOR KUZNETSOV, DAVID EMM,

MARC RIVERO, DAN DEMETER,

SHERIF MAGDY

CYBERTHREAT TALKS

09 NOV 2023, 5:00PM 60 MIN

Overview of modern car compromise techniques and methods of protection

ALEXANDER KOZLOV,

SERGEY ANUFRIENKO

// REPORTS

HrServ – Previously unknown web shell used in APT attack

In this report Kaspersky researchers provide an analysis of the previously unknown HrServ web shell, which exhibits both APT and crimeware features and has likely been active since 2021.

A cascade of compromise: unveiling Lazarus' new campaign

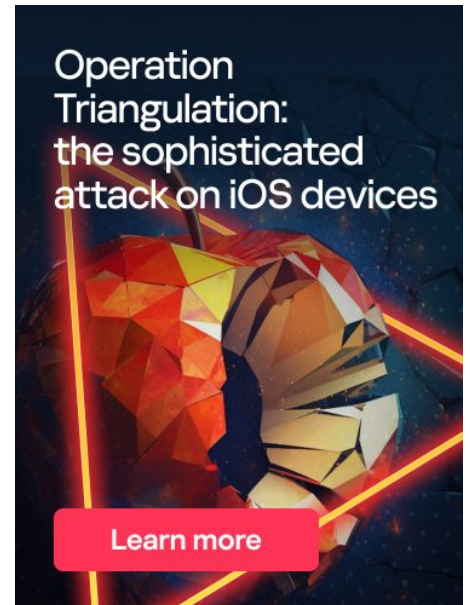
We unveil a Lazarus campaign exploiting security company products and examine its intricate connections with other campaigns

Modern Asian APT groups' tactics, techniques and procedures (TTPs)

Asian APT groups target various organizations from a multitude of regions and industries. We created this report to provide the cybersecurity community with the best-prepared intelligence data to effectively counteract Asian APT groups.

How to catch a wild triangle

How Kaspersky researchers obtained all stages of the Operation Triangulation campaign targeting iPhones and iPads, including zero-day exploits, validators, TriangleDB implant and additional modules.



// SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

[Subscribe](#)☐

I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

THREATS

APT (Targeted attacks)
Secure environment (IoT)
Mobile threats
Financial threats
Spam and phishing
Industrial threats
Web threats
Vulnerabilities and exploits

CATEGORIES

APT reports
Malware descriptions
Security Bulletin
Malware reports
Spam and phishing reports
Security technologies
Research
Publications

OTHER SECTIONS

Archive
All tags
Webinars
APT Logbook
Statistics
Encyclopedia
Threats descriptions
KSB 2023

© 2024 AO Kaspersky Lab. All Rights Reserved.

Registered trademarks and service marks are the property of their respective owners.

Privacy Policy
Cookies

License Agreement