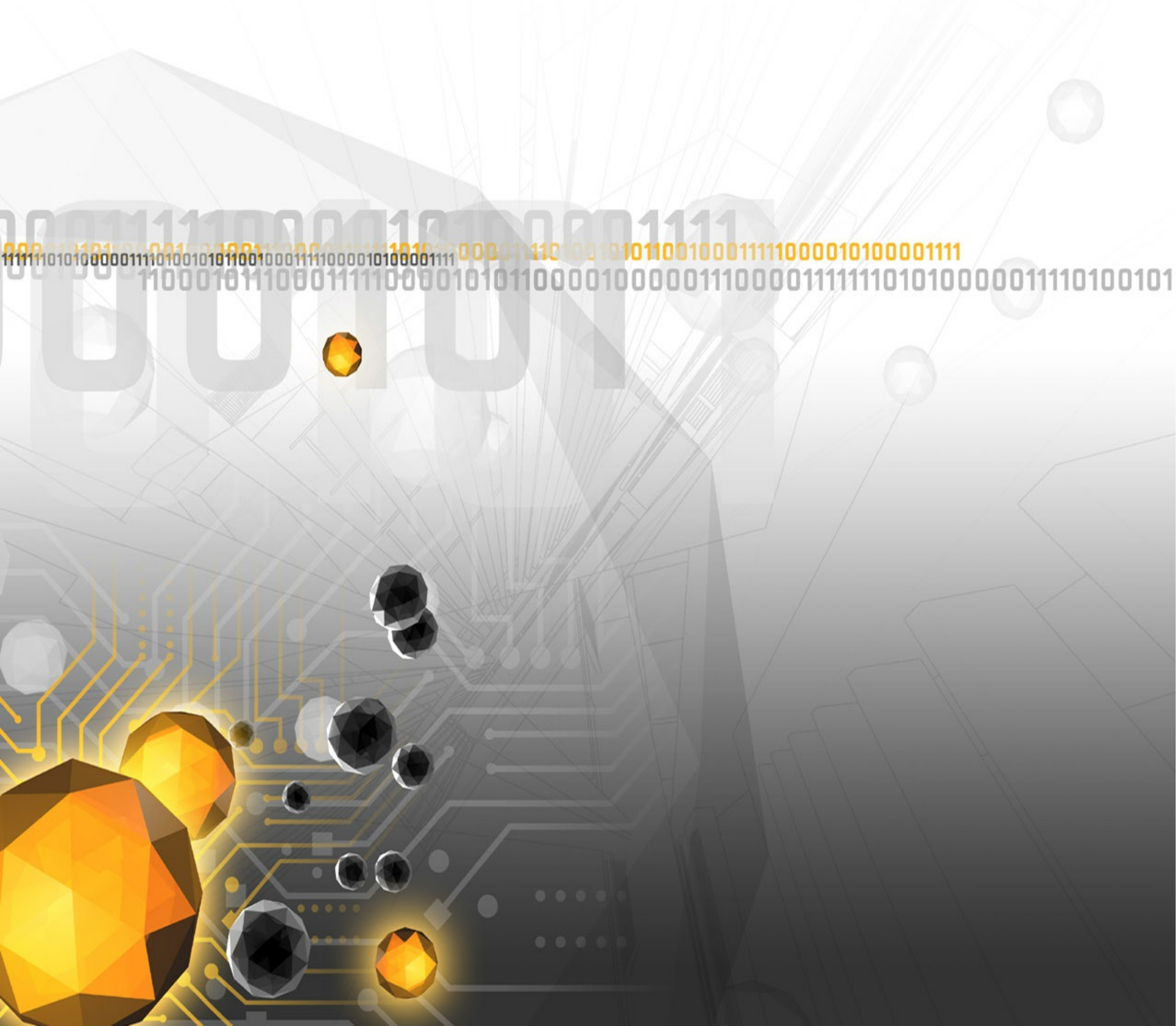
TROJAN.JECTIN USED TO TARGET PRO-ISRAEL ORGANIZATIONS

MANAGED ADVERSARY AND THREAT INTELLIGENCE

DEEPSIGHT™ INTELLIGENCE | INTELLIGENCE REPORT | SYMC - 300246 | V.1
05 AUG 2015 GMT



LEGAL NOTICE

SYMANTEC PROPRIETARY & CONFIDENTIAL - PERMITTED USE ONLY

This document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any, except that authorized customers of Symantec's DeepSight™ Intelligence services may use this document only for internal purposes in accordance with their DeepSight™ Intelligence services agreement.

Symantec assigns a high, medium, or low degree of confidence to assessments within its DeepSight™ Intelligence Portal Managed Adversary and Threat Intelligence (MATI) products. Confidence levels are determined against a three-point spectrum of source validity: variety and non-conflictive disparity of original sources, quality of source reporting, and reliability of source reporting. Confidence levels may be increased based on independent corroboration of information. High confidence generally suggests a solid judgment can be made, though such a judgment carries the risk of being wrong. Low confidence generally suggests tenuous inferences can be made, though information used to do so may have been questionable, fragmented, or singular.

THIS DOCUMENT IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENT. THE INFORMATION CONTAINED IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE.

Information Cut-Off Date: 03 Aug 2015 GMT

Trojan.Jectin Used to Target Pro-Israel Organizations

DeepSight™ Intelligence | Intelligence Report | SYMC - 300246 | V.1 | 05 Aug 2015 GMT

KEY FINDINGS

A cyber espionage campaign targeted three pro-Israel organizations between 4 February and 21 April 2015.

Targeting characteristics used in the campaign were consistent with those from a group with nation-state aligned goals and regional interests in the Middle East.

DeepSight Intelligence observed additional domains impersonating Microsoft services with the same registrant information. These domains could be used to support future attack operations.

EXECUTIVE SUMMARY

A cyber espionage campaign targeting pro-Israel organizations used the recently discovered malware Trojan.Jectin in February and April 2015. The campaign lured the recipients with crafted emails and themes related to the Israel Ministry of Foreign Affairs (MFA) and the United Nations. Based on the narrow targeting, Hebrew language traits, and functionality of the malware, the intent was likely to gather information related to pro-Israeli advocacy activities. While the operation did demonstrate focus on a very specific target set, the execution of the targeting indicates that this attack group is inexperienced or lacks the resources to be highly adaptable.

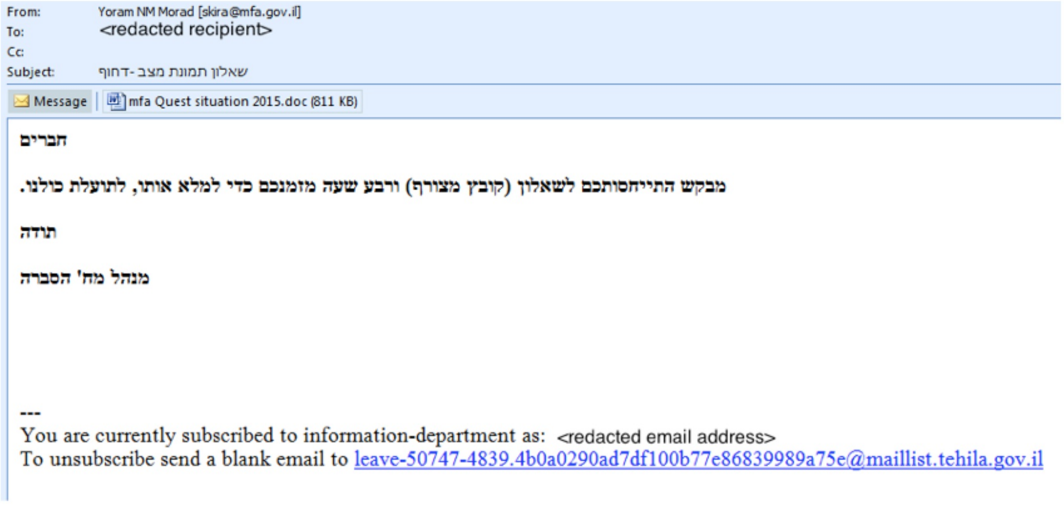
DETAILS

Between 4 February and 21 April 2015, DeepSight Intelligence observed a cyber espionage campaign against three organizations involved in pro-Israel political advocacy activities—two in Israel and one in the United States. Based on the targeting, it is likely the motivation of this campaign was to gather sensitive information pertaining to Israel. While these targeting objectives appear consistent with actors with nation-state allegiance, it was also conducted by actors with apparently limited operational capabilities.

Israeli Ministry of Foreign Affairs Questionnaire

This campaign used crafted emails containing topics involving either the United Nations Conference or the Israeli Ministry of Foreign Affairs to deliver the information stealing malware (Trojan.Jectin)[1]. Trojan.Jectin has not been associated with any widespread cyber activities and was almost certainly controlled by a single group at the time of this campaign.

Figure 1 shows the Hebrew-language email that DeepSight Intelligence observed on 9 February 2015 containing the malicious Microsoft Word file attachment (MD5: 4765369D8AE52F2DD9B318E0C8B27054).



From: Yoram NM Morad [skira@mfa.gov.il]
To: <redacted recipient>
Cc:
Subject: שאלון תמונת מצב -דחוף

חברים

מבקש התייחסותכם לשאלון (קובץ מצורף) ורבע שעה מזמנכם כדי למלא אותו, לתועלת כולנו.

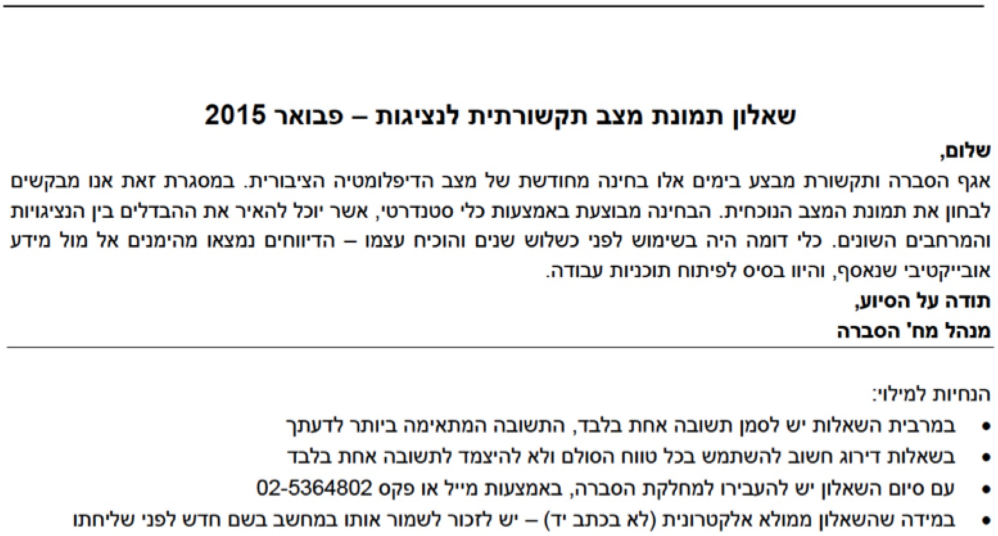
תודה

מנהל מח' הסברה

You are currently subscribed to information-department as: <redacted email address>
To unsubscribe send a blank email to leave-50747-4839.4b0a0290ad7df100b77e86839989a75e@maillist.tehila.gov.il

Figure 1. Hebrew language email sent on 9 February 2015

Contained within this Word file is the Trojan.Jectin portable executable (PE) that communicates with the domain u.mywindows24[.]in. Furthermore, the PE launches a decoy PDF file with Hebrew language contents (see Figure 2).



שאלון תמונת מצב תקשורתית לנציגות – פבואר 2015

שלום,

אגף הסברה ותקשורת מבצע בימים אלו בחינה מחודשת של מצב הדיפלומטיה הציבורית. במסגרת זאת אנו מבקשים לבחון את תמונת המצב הנוכחית. הבחינה מבוצעת באמצעות כלי סטנדרטי, אשר יוכל להאיר את ההבדלים בין הנציגויות והמרחבים השונים. כלי דומה היה בשימוש לפני כשלוש שנים והוכיח עצמו – הדיווחים נמצאו מהימנים אל מול מידע אובייקטיבי שנאסף, והיוו בסיס לפיתוח תוכניות עבודה.

תודה על הסיוע,

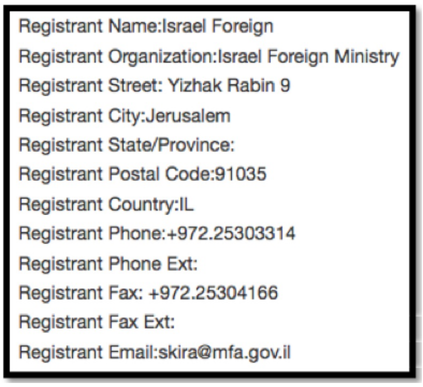
מנהל מח' הסברה

הנחיות למילוי:

- במרבית השאלות יש לסמן תשובה אחת בלבד, התשובה המתאימה ביותר לדעתך
- בשאלות דירוג חשוב להשתמש בכל טווח הסולם ולא להיצמד לתשובה אחת בלבד
- עם סיום השאלון יש להעבירו למחלקת הסברה, באמצעות מייל או פקס 02-5364802
- במידה שהשאלון ממולא אלקטרונית (לא בכתב יד) – יש לזכור לשמור אותו במחשב בשם חדש לפני שליחתו

Figure 2. Excerpt from the decoy PDF document launched by the Trojan.Jectin PE

The email likely used a spoofed sender email address to impersonate Yoram Morad, the Director of the Department of Digital Diplomacy for the Israel Ministry of Foreign Affairs (MFA). The email address observed in this targeting, skira[@]mfa.gov.il, has been publicly associated with the registration of the domain Israel[.]org, a MFA website, but not specifically with Yoram Morad.

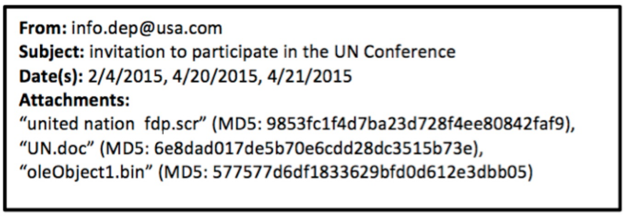


```
Registrant Name:Israel Foreign
Registrant Organization:Israel Foreign Ministry
Registrant Street: Yizhak Rabin 9
Registrant City:Jerusalem
Registrant State/Province:
Registrant Postal Code:91035
Registrant Country:IL
Registrant Phone:+972.25303314
Registrant Phone Ext:
Registrant Fax: +972.25304166
Registrant Fax Ext:
Registrant Email:skira@mfa.gov.il
```

Figure 3. Registrant information for Israel[.]org

United Nations Conference Invitation

On 4 February, 20 April, and 21 April 2015, emails sent from info.dep[@]usa.com targeted three organizations involved in Pro-Israel initiatives—two based in Israel and one in the United States. The email domain "usa[.]com" can be obtained using a free email service and was likely created by the attack group. Using a United Nations theme, the targeted email sought to convince the recipient to execute a payload, which has been determined to be Trojan.Jectin.



From: info.dep@usa.com
Subject: invitation to participate in the UN Conference
Date(s): 2/4/2015, 4/20/2015, 4/21/2015
Attachments:
"united nation fdp.scr" (MD5: 9853fc1f4d7ba23d728f4ee80842faf9),
"UN.doc" (MD5: 6e8dad017de5b70e6cdd28dc3515b73e),
"oleObject1.bin" (MD5: 577577d6df1833629bfd0d612e3dbb05)

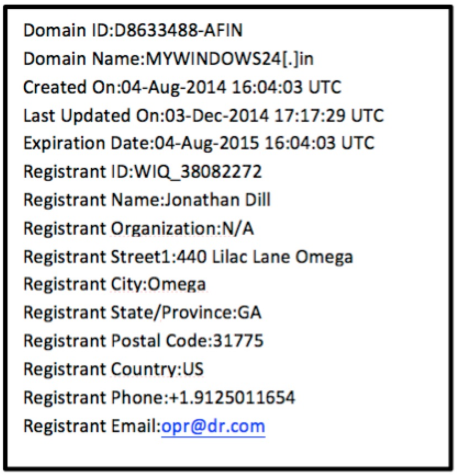
Figure 4. Details of the United Nations-themed email

A fourth organization, a France-based financial institution, was also targeted in the campaign. While this organization is not a pro-Israel organization, its prior involvement in United Nations projects could have been the reason it was targeted.

The emails used during the course of this operation included three different attachment types: DOC, SCR, and BIN. Each of the four unique targeted email addresses received two separate emails containing different attachments. This persistent trial-and-error use of attachment types likely indicates repeated attempts after previous targeted emails failed. The file attachment oleObject1.bin, which was used in the 20 and 21 April emails, is the payload from the attachment UN.doc (MD5: 6e8dad017de5b70e6cdd28dc3515b73e).

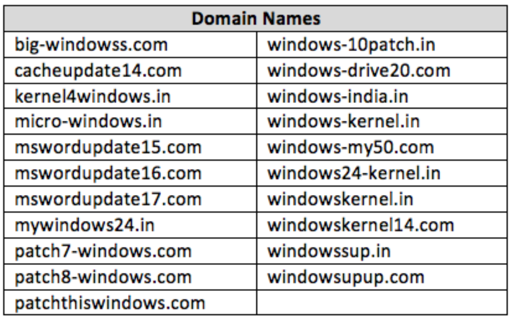
Possible Trojan.Jectin-Related Infrastructure

Network infrastructure associated with known Trojan.Jectin variants includes windowslayer[.]in, u.mywindows24[.]in, main.windowskernel14[.]com, and 209[.]190.20.59. Additionally, two of the three domains associated with the Trojan.Jectin family (Figure 5) were registered by Jonathan Dill (opr[@]dr.com). Several other domains that impersonate Microsoft-related sites have been registered with the same information (see Figure 6). While these domains have not been observed in connection to this campaign or to Trojan.Jectin, it is possible that they were intended to support further activity related to this malware.



Domain ID:D8633488-AFIN
Domain Name:MYWINDOWS24[.]in
Created On:04-Aug-2014 16:04:03 UTC
Last Updated On:03-Dec-2014 17:17:29 UTC
Expiration Date:04-Aug-2015 16:04:03 UTC
Registrant ID:WIQ_38082272
Registrant Name:Jonathan Dill
Registrant Organization:N/A
Registrant Street1:440 Lilac Lane Omega
Registrant City:Omega
Registrant State/Province:GA
Registrant Postal Code:31775
Registrant Country:US
Registrant Phone:+1.9125011654
Registrant Email:opr@dr.com

Figure 5. Registrant information for the domain mywindows24[.]in



Domain Names	
big-windowss.com	windows-10patch.in
cacheupdate14.com	windows-drive20.com
kernel4windows.in	windows-india.in
micro-windows.in	windows-kernel.in
mswordupdate15.com	windows-my50.com
mswordupdate16.com	windows24-kernel.in
mswordupdate17.com	windowskernel.in
mywindows24.in	windowskernel14.com
patch7-windows.com	windowssup.in
patch8-windows.com	windowsupup.com
patchthiswindows.com	

Figure 6. Domains registered by Jonathan Dill (opr[@]dr.com)

[1] Trojan.Jectin was first reported by Symantec on 9 April 2015 as malware capable of the collection and exfiltration of screenshots, keystrokes, and email configuration and credential information.

OUTLOOK

This operation was characterized by the low-volume pursuit of specific strategic targets that is often associated with groups that seek sensitive information. In this case, the focus on pro-Israel organizations suggests the group's alignment with the national intelligence needs of a Middle-Eastern country. Organizations associated with high-profile, pro-Israel activities will remain probable targets for groups with these motivations, which includes the attack group associated with this activity and well-documented cyber espionage groups such as the likely Iranian group ATG9 (a.k.a. Rocket Kitten).

The tactics and lure files used in this operation revealed the group's low level of adaptability and skill in the execution of this operation. This is most prominently highlighted by the use of previously developed resources when the payload oleObject1.bin was directly attached to the email instead of as part of a newly crafted lure document. DeepSight Intelligence expects that this group will struggle to overcome the detectability of Trojan.Jectin and require more time than more adept cyber espionage groups to continue this campaign.

TECHNICAL DETAILS

See the ***Metadata*** tab for additional technical details related to this report.

METADATA

CAMPAIGNS

Name	ID	Status
UNK001-CE.0074	CE.0074	Unknown

EXTRACTED INDICATORS

Indicator	Indicator Related CVE	Indicator Type
big-windowss.com		domain
cacheupdate14.com		domain
kernel4windows.in		domain
micro-windows.in		domain
mswordupdate15.com		domain
mswordupdate16.com		domain
mswordupdate17.com		domain
mywindows24.in		domain
patch7-windows.com		domain
patch8-windows.com		domain
patchthiswindows.com		domain
windows-10patch.in		domain
windows-drive20.com		domain
windows-india.in		domain
windows-kernel.in		domain
windows-my50.com		domain
windows24-kernel.in		domain
windowskernel.in		domain
windowskernel14.com		domain
windowssup.in		domain
windowsupup.com		domain
http://u.mywindows24.in/img/513e94bb4b6b695c014b6b6d32840016/9b4eb90ed3d75b4a8/general.png		url
u.mywindows24.in		domain
windowslayer.in		domain
u.mywindows24.in		domain

Indicator	Indicator Related CVE	Indicator Type
main.windowskernel14.com		domain
209.190.20.59		ip_address
info.dep@usa.com		email_from_address
http://u.mywindows24.in/img/%s/8544b90ed3d7673a1/n%d.png		url
http://u.mywindows24.in/img/%s/8544b90ed3d7673a1/general.png		url
united-nation??fdp.scr		file_name
9853fc1f4d7ba23d728f4ee80842faf9		file_md5
ee01d0926b80695ca6413e97ff4e824ada0f09fced5ecd00231c7e287336b112		file_sha256
6e8dad017de5b70e6cdd28dc3515b73e		file_md5
70788c7037e4c59bc791a93e075013db15789003e800cfe678212274d43e00fc		file_sha256
577577d6df1833629bfd0d612e3dbb05		file_md5
2df6fe9812796605d4696773c91ad84c4c315df7df9cf78bee5864822b1074c9		file_sha256
4765369D8AE52F2DD9B318E0C8B27054		file_md5
9DB2719A3DDE09AE260DEF9CD0D46DBE		file_md5
9701370e99061f9e4ad963c2229361edf5b963c880dc51d7ac4702438f98fdff		file_sha256
9DB2719A3DDE09AE260DEF9CD0D46DBE		file_md5
9701370e99061f9e4ad963c2229361edf5b963c880dc51d7ac4702438f98fdff		file_sha256
pdedeac.tmp		file_name
t20249215284695.exe		file_name
1cef128513c05837f24796042b8e1cd9		file_md5
696f7da3858ab101b8493e925054cfd88a3ddb6956677cfa785bf35cfbf818ac		file_sha256
C5ADE105206A6A265F66747C6ABB63E0		file_md5
un.doc		file_name
e9297882232f196794f16c1b063c5d3835676183880d7f292e2109494540355b		file_sha256
A9302B4FA8F00BCC044D30A0FC10DFED		file_md5
a3739a296b70434dc4800445958b3d3849cca22a2a2f20a8eee007ed3b20134c		file_sha256
54D41904F1298563DC794A223C42CB79		file_md5
dfa027e31f0cf783af0212aad6e192202b55eaac4af0b3cc87ece6389fcfc1ee		file_sha256
injector.dll		file_name
3468C1EE32B0B6B736372697C78354BE		file_md5
209a195c6c20ccad3b9ca302f6fc97d838df2eddf9d5b4cfc6a45cf5f55e7d7c		file_sha256
DA3C3CCA0FC749D5686D09D03B855714		file_md5
1f98d888550e2292366c6f687feb9d8a37ca760df6d50079919e013de165f9a7		file_sha256
EC13C4ECE6C5C70D4F30402A1E424FAD		file_md5
3c100d54a18853014689ba8dddb55a1f46351aaffed2451a8a4a42f7751fb912		file_sha256
969926B06119ADA19E297D600DBB61ED		file_md5

Indicator	Indicator Related CVE	Indicator Type
56c44513b3c569ce0b2544fa5c454aa219fc3bafae990f7fe7301801e6cd5896		file_sha256
2D80F339B6CD0E6FFDFBA7D442FFEC90		file_md5
de26748d750b99aac8a2b55595341d1095eb5010f5c48cf5dd365dc3afc4a324		file_sha256
update5x.zip		file_name
2F0C8B31035DA503AF9E141DBB0C74CD		file_md5
update.zip		file_name
002d4dfc09a6f45e81245bc43ec64b2a4d89227c8bf5e027df95bad3449b91e8		file_sha256
71463E5D565B1BAC36F3BC187D8F3940		file_md5
cd89407c0a157604d1e34c12dc99bff3991d4493a5d884fa133f8d1a4a5fd0a5		file_sha256
DA8F80B01B0E2361A66A628A77D54E8E		file_md5
c84d739714fc86f5ad33973c85a36573ee636ec892e12e749a1279a2344b7237		file_sha256
44B3882CB9C04F532C78544F20F15E49		file_md5
55b6f73cb9da5ae65fcedf952e94917ef5342249595e39d3a56642cbbe50f255		file_sha256
4D4A85BA414505DEFB1A3DB03279D964		file_md5
74a57835857b94fed433ea16785ed9ef43501f2bfaf05558c778a8f76f413b20		file_sha256
A2479CD72C7295FA68D51F3C3D3E2A2E		file_md5
e06c2688a5e20979bdc197ce2fdcf06425de0ef72ee2a38361aa605d16130007		file_sha256
9853fc1f4d7ba23d728f4ee80842faf9		file_md5
ee01d0926b80695ca6413e97ff4e824ada0f09fced5ecd00231c7e287336b112		file_sha256
6e8dad017de5b70e6cdd28dc3515b73e		file_md5
70788c7037e4c59bc791a93e075013db15789003e800cfe678212274d43e00fc		file_sha256
577577d6df1833629bfd0d612e3dbb05		file_md5
2df6fe9812796605d4696773c91ad84c4c315df7df9cf78bee5864822b1074c9		file_sha256
4765369D8AE52F2DD9B318E0C8B27054		file_md5
ab7c0e80821efbdacb73800ba28b85f1b6fc5e2bb1359eb12f9fc0dc063e5006		file_sha256
9DB2719A3DDE09AE260DEF9CD0D46DBE		file_md5
9701370e99061f9e4ad963c2229361edf5b963c880dc51d7ac4702438f98fdff		file_sha256
9DB2719A3DDE09AE260DEF9CD0D46DBE		file_md5
9701370e99061f9e4ad963c2229361edf5b963c880dc51d7ac4702438f98fdff		file_sha256
1cef128513c05837f24796042b8e1cd9		file_md5
696f7da3858ab101b8493e925054cfd88a3ddb6956677cfa785bf35cfbf818ac		file_sha256
C5ADE105206A6A265F66747C6ABB63E0		file_md5
e9297882232f196794f16c1b063c5d3835676183880d7f292e2109494540355b		file_sha256
A9302B4FA8F00BCC044D30A0FC10DFED		file_md5
a3739a296b70434dc4800445958b3d3849cca22a2a2f20a8eee007ed3b20134c		file_sha256
54D41904F1298563DC794A223C42CB79		file_md5

Indicator	Indicator Related CVE	Indicator Type
dfa027e31f0cf783af0212aad6e192202b55eaac4af0b3cc87ece6389fcfc1ee		file_sha256
3468C1EE32B0B6B736372697C78354BE		file_md5
209a195c6c20ccad3b9ca302f6fc97d838df2eddf9d5b4cfc6a45cf5f55e7d7c		file_sha256
DA3C3CCA0FC749D5686D09D03B855714		file_md5
1f98d888550e2292366c6f687feb9d8a37ca760df6d50079919e013de165f9a7		file_sha256
EC13C4ECE6C5C70D4F30402A1E424FAD		file_md5
3c100d54a18853014689ba8dddb55a1f46351aaffed2451a8a4a42f7751fb912		file_sha256
969926B06119ADA19E297D600DBB61ED		file_md5
56c44513b3c569ce0b2544fa5c454aa219fc3bafae990f7fe7301801e6cd5896		file_sha256
2D80F339B6CD0E6FFDFBA7D442FFEC90		file_md5
de26748d750b99aac8a2b55595341d1095eb5010f5c48cf5dd365dc3afc4a324		file_sha256
2F0C8B31035DA503AF9E141DBB0C74CD		file_md5
002d4dfc09a6f45e81245bc43ec64b2a4d89227c8bf5e027df95bad3449b91e8		file_sha256
71463E5D565B1BAC36F3BC187D8F3940		file_md5
cd89407c0a157604d1e34c12dc99bff3991d4493a5d884fa133f8d1a4a5fd0a5		file_sha256
DA8F80B01B0E2361A66A628A77D54E8E		file_md5
c84d739714fc86f5ad33973c85a36573ee636ec892e12e749a1279a2344b7237		file_sha256
44B3882CB9C04F532C78544F20F15E49		file_md5
55b6f73cb9da5ae65fcedf952e94917ef5342249595e39d3a56642cbbe50f255		file_sha256
4D4A85BA414505DEFB1A3DB03279D964		file_md5
74a57835857b94fed433ea16785ed9ef43501f2bfaf05558c778a8f76f413b20		file_sha256
A2479CD72C7295FA68D51F3C3D3E2A2E		file_md5
e06c2688a5e20979bdc197ce2fdcf06425de0ef72ee2a38361aa605d16130007		file_sha256

FILES

Detection Name	Name	MD5	SHA 256	Malicious
Trojan.Asprox.B,SONAR.ProcHijack!gen5,SONAR.ProcHijack!gen1	united-nation??fdp.scr	9853fc1f4d7ba23d728f4ee80842faf9	ee01d0926b80695ca6413e97ff4e824ada0f09fced5ecd00231c7e287336b112	y
Trojan.Asprox.B	un.doc	6e8dad017de5b70e6cdd28dc3515b73e	70788c7037e4c59bc791a93e075013db15789003e800cfe678212274d43e00fc	y
		577577d6df1833629bfd0d612e3dbb05	2df6fe9812796605d4696773c91ad84c4c315df7df9cf78bee5864822b1074c9	y
Trojan.Mdropper		4765369D8AE52F2DD9B318E0C8B27054	ab7c0e80821efbdacb73800ba28b85f1b6fc5e2bb1359eb12f9fc0dc063e5006	y

Detection Name	Name	MD5	SHA 256	Malicious
Downloader.Ponik	pdedeac.tmp	9DB2719A3DDE09AE260DEF9CD0D46DBE	9701370e99061f9e4ad963c2229361edf5b963c880dc51d7ac4702438f98fdff	y
Downloader.Ponik	pdedeac.tmp	9DB2719A3DDE09AE260DEF9CD0D46DBE	9701370e99061f9e4ad963c2229361edf5b963c880dc51d7ac4702438f98fdff	y
Trojan.Jectin,Trojan Horse	t20249215284695.exe	1cef128513c05837f24796042b8e1cd9	696f7da3858ab101b8493e925054cfd88a3ddb6956677cfa785bf35cfbf818ac	y
Trojan.Jectin		C5ADE105206A6A265F66747C6ABB63E0	e9297882232f196794f16c1b063c5d3835676183880d7f292e2109494540355b	y
Trojan.Jectin	update5x.zip	A9302B4FA8F00BCC044D30A0FC10DFED	a3739a296b70434dc4800445958b3d3849cca22a2a2f20a8eee007ed3b20134c	y
Trojan.Jectin		54D41904F1298563DC794A223C42CB79	dfa027e31f0cf783af0212aad6e192202b55eaac4af0b3cc87ece6389fcfc1ee	y
Trojan.Jectin	injector.dll	3468C1EE32B0B6B736372697C78354BE	209a195c6c20ccad3b9ca302f6fc97d838df2eddf9d5b4cfc6a45cf5f55e7d7c	y
Trojan.Jectin	injector.dll	DA3C3CCA0FC749D5686D09D03B855714	1f98d888550e2292366c6f687feb9d8a37ca760df6d50079919e013de165f9a7	y
Trojan.Jectin	injector.dll	EC13C4ECE6C5C70D4F30402A1E424FAD	3c100d54a18853014689ba8dddb55a1f46351aaffed2451a8a4a42f7751fb912	y
Trojan.Jectin	injector.dll	969926B06119ADA19E297D600DBB61ED	56c44513b3c569ce0b2544fa5c454aa219fc3bafae990f7fe7301801e6cd5896	y
Trojan.Jectin		2D80F339B6CD0E6FFDFBA7D442FFEC90	de26748d750b99aac8a2b55595341d1095eb5010f5c48cf5dd365dc3afc4a324	y
Trojan.Jectin	injector.dll	2F0C8B31035DA503AF9E141DBB0C74CD	002d4dfc09a6f45e81245bc43ec64b2a4d89227c8bf5e027df95bad3449b91e8	y
Trojan.Jectin	update5x.zip	71463E5D565B1BAC36F3BC187D8F3940	cd89407c0a157604d1e34c12dc99bff3991d4493a5d884fa133f8d1a4a5fd0a5	y
Trojan.Jectin	update.zip	DA8F80B01B0E2361A66A628A77D54E8E	c84d739714fc86f5ad33973c85a36573ee636ec892e12e749a1279a2344b7237	y
Trojan.Jectin	injector.dll	44B3882CB9C04F532C78544F20F15E49	55b6f73cb9da5ae65fcedf952e94917ef5342249595e39d3a56642cbbe50f255	y
Trojan.Jectin	update5x.zip	4D4A85BA414505DEFB1A3DB03279D964	74a57835857b94fed433ea16785ed9ef43501f2bfaf05558c778a8f76f413b20	y

Detection Name	Name	MD5	SHA 256	Malicious
Trojan.Jectin	injector.dll	A2479CD72C7295FA68D51F3C3D3E2A2E	e06c2688a5e20979bdc197ce2fdcf06425de0ef72ee2a38361aa605d16130007	y
Trojan.Asprox.B,SONAR.ProcHijack!gen5,SONAR.ProcHijack!gen1	united-nation??fdp.scr	9853fc1f4d7ba23d728f4ee80842faf9	ee01d0926b80695ca6413e97ff4e824ada0f09fced5ecd00231c7e287336b112	y
Trojan.Asprox.B	un.doc	6e8dad017de5b70e6cdd28dc3515b73e	70788c7037e4c59bc791a93e075013db15789003e800cfe678212274d43e00fc	y
None		577577d6df1833629bfd0d612e3dbb05	2df6fe9812796605d4696773c91ad84c4c315df7df9cf78bee5864822b1074c9	y
Downloader.Ponik,Trojan.Mdropper	ab7c0e80821efbdacb73800ba28b85f1b6fc5e2bb1359eb12f9fc0dc063e5006	4765369D8AE52F2DD9B318E0C8B27054	ab7c0e80821efbdacb73800ba28b85f1b6fc5e2bb1359eb12f9fc0dc063e5006	y
Downloader.Ponik	pdedeac.tmp	9DB2719A3DDE09AE260DEF9CD0D46DBE	9701370e99061f9e4ad963c2229361edf5b963c880dc51d7ac4702438f98fdff	y
Downloader.Ponik	pdedeac.tmp	9DB2719A3DDE09AE260DEF9CD0D46DBE	9701370e99061f9e4ad963c2229361edf5b963c880dc51d7ac4702438f98fdff	y
Trojan.Jectin,Trojan Horse	t20249215284695.exe	1cef128513c05837f24796042b8e1cd9	696f7da3858ab101b8493e925054cfd88a3ddb6956677cfa785bf35cfbf818ac	y
Trojan.Jectin		C5ADE105206A6A265F66747C6ABB63E0	e9297882232f196794f16c1b063c5d3835676183880d7f292e2109494540355b	y
Trojan.Jectin	update5x.zip	A9302B4FA8F00BCC044D30A0FC10DFED	a3739a296b70434dc4800445958b3d3849cca22a2a2f20a8eee007ed3b20134c	y
Trojan.Jectin		54D41904F1298563DC794A223C42CB79	dfa027e31f0cf783af0212aad6e192202b55eaac4af0b3cc87ece6389fcfc1ee	y
Trojan.Jectin	injector.dll	3468C1EE32B0B6B736372697C78354BE	209a195c6c20ccad3b9ca302f6fc97d838df2eddf9d5b4cfc6a45cf5f55e7d7c	y
Trojan.Jectin	injector.dll	DA3C3CCA0FC749D5686D09D03B855714	1f98d888550e2292366c6f687feb9d8a37ca760df6d50079919e013de165f9a7	y
Trojan.Jectin	injector.dll	EC13C4ECE6C5C70D4F30402A1E424FAD	3c100d54a18853014689ba8dddb55a1f46351aaffed2451a8a4a42f7751fb912	y
Trojan.Jectin	injector.dll	969926B06119ADA19E297D600DBB61ED	56c44513b3c569ce0b2544fa5c454aa219fc3bafae990f7fe7301801e6cd5896	y
Trojan.Jectin		2D80F339B6CD0E6FFDFBA7D442FFEC90	de26748d750b99aac8a2b55595341d1095eb5010f5c48cf5dd365dc3afc4a324	y

Detection Name	Name	MD5	SHA 256	Malicious
Trojan.Jectin	injector.dll	2F0C8B31035DA503AF9E141DBB0C74CD	002d4dfc09a6f45e81245bc43ec64b2a4d89227c8bf5e027df95bad3449b91e8	y
Trojan.Jectin	update5x.zip	71463E5D565B1BAC36F3BC187D8F3940	cd89407c0a157604d1e34c12dc99bff3991d4493a5d884fa133f8d1a4a5fd0a5	y
Trojan.Jectin	update.zip	DA8F80B01B0E2361A66A628A77D54E8E	c84d739714fc86f5ad33973c85a36573ee636ec892e12e749a1279a2344b7237	y
Trojan.Jectin	injector.dll	44B3882CB9C04F532C78544F20F15E49	55b6f73cb9da5ae65fcedf952e94917ef5342249595e39d3a56642cbbe50f255	y
Trojan.Jectin	update5x.zip	4D4A85BA414505DEFB1A3DB03279D964	74a57835857b94fed433ea16785ed9ef43501f2bfaf05558c778a8f76f413b20	y
Trojan.Jectin	injector.dll	A2479CD72C7295FA68D51F3C3D3E2A2E	e06c2688a5e20979bdc197ce2fdcf06425de0ef72ee2a38361aa605d16130007	y

TARGET INDUSTRIES

NAICS Code	Name
92	Public Administration
52	Finance and Insurance

TARGET REGIONS

Region	Americas; Asia; Europe
Subregion	North America; Western Asia; Western Europe
Countries	United States; Israel; France

THREAT DOMAINS

Cyber Espionage