

**מטלת הגשה מסכמת**

**"הנדסה לאחור וניתוח תוכנות זדוניות"**

סמסטר קיץ 2020

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **נייד** | **מייל** | **ת.ז** | **שם מלא באנגלית** | **שם מלא בעברית** |  |
| *054-5884399* | *OfekPintok@gmail.com* | *308409267* | *Ofek Pintok* | *אופק פינטוק* | *1* |
| *054-7696933* | *HenSomeh@gmail.com* | *313468654* | *Hen Haim Someh* | *חן חיים סומך* | *2* |

**מטלה 1: נוזקות מורכבות**

במטלה זו בחרנו לעסוק בנוזקה בשם ZeuS כחלק ממשפחת ZBOT.

**התייחסות היסטורית ורקע כללי**

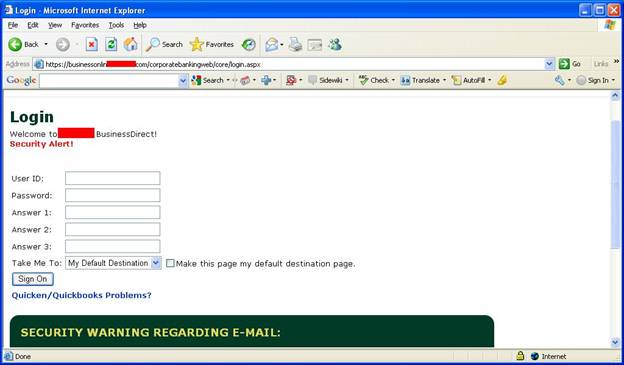
ZeuS botnet הוא מונח מקוצר לרשתות מחשבים שנמצאים בסכנה המשתמשת בעזרת סוסים טרויאניים של ZeuS/ZBOT בפעולות שונות הקשורות לבוט-נט.  
הנוזקה מגיעה בדרך כלל באמצעות דואר זבל שנראה שמקורן לגיטימי ומבקשות מהנמענים ללחוץ על קישור.  
הקישור האמור מוביל להורדת TSPY\_ZBOT, אשר יושב בשקט במערכות ומחכה שאותם הקורבנות יזינו את תעודותיהם ופרטיהם האישיים לאתרים מסוימים.  
משפחת הנוזקה ZBOT התגלתה על ידי חברה בשם Trend Micro בשנת 2007, ובמהלך השנים גילו עוד ועוד נוזקות הקשורות למשפחה זו.  
נכון להיום, התגלו למעלה מ-2000 נוזקות שונות הקשורות למשפחה זו והמספר ממשיך לעלות.

**פירוט טכני**

המטרה לשמה נועדה הנוזקה הינה לגנוב פרטים או חשבונות משתמשים ממגוון אתרים לדוגמא: מערכות בנק אונליין, רשתות חברתיות ואתרי מסחר אלקטרוניים.  
ZeuS מבצע סינון נתונים ופקודות מרחוק באמצעות בקשותHTTP POST מוצפנות לשרת אינטרנט של שליטה ובקשה.  
ההצפנה בה משתמשת הנוזקה היא RC4 עם מפתח המוטמע בבינארי.  
ניתן לבצע כמה ממשימות אלה "לפי דרישה" באמצעות לוח הבקרה המבוסס HTTP, ולהפנות אותן למחשבים נגועים שנבחרו. משימות "לפי דרישה" עשויות להתבצע באמצעות סקריפטים מיוחדים שניתן לבצע במערכות נבחרות. ניתן להשתמש בסקריפטים אלה בכדי לקחת צילומי מסך של מערכות נגועות או לביצוע עדכונים של הנוזקה עצמה.

Graphical user interface, text, application, email

Description automatically generated  
*תמונה 1: מבט על דף התחברות לאתר פיננסי*

  
*תמונה 2: מבט על אותו הדף אך ממחשב נגוע ב-ZeuS, שימו לב כי הוא מכיל 3 שדות חדשים*

בנוסף, ZeuS בעל יכולות לבצע סליקה אוטומטית (ACH). ACH הינה רשת אלקטרונית רחבה לביצוע עסקאות פיננסיות בארצות הברית. המערכת משמשת לתשלומי חשבונות מקוונים, הפקדת שכר ישירות ממעסיקים, העברת כסף בין חשבונות וכו'.  
הנוזקה מותקנות על מחשבים פוטנציאליים ובהם מותקנים קבצים ותיקיות שלרוב יהיו בעלי תכונת “Hidden” אשר מסתירה אותה מבדיקות סתמיות.

מיקום הקבצים תלוי האם למחשב הקורבן יש הרשאות מנהל או לא.

עם הרשאות אדמיניסטרציה:

*%systemroot%\system32\sdra64.exe (malware)  
%systemroot%\system32\lowsec  
%systemroot%\system32\lowsec\user.ds (encrypted stolen data file) %systemroot%\system32\lowsec\user.ds.lll (temporary file for stolen data) %systemroot%\system32\lowsec\local.ds (encrypted configuration file)*

ללא הרשאות אדמיניסטרציה:

*%appdata%\sdra64.exe  
%appdata%\lowsec  
%appdata%\lowsec\user.ds  
%appdata%\lowsec\user.ds.lll  
%appdata%\lowsec\local.ds*

בדרך כלל ZeuS יבצע שינויים בעת "רישומו" למערכת בכדי להבטיח שהוא יופעל מחדש בכל פעם.  
  
עם הרשאות אדמיניסטרציה:

*HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon  
From:  
"Userinit" = "C:\WINDOWS\system32\userinit.exe"  
To:  
"Userinit" = "C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe"*

ללא הרשאות אדמיניסטרציה:

*HKCU\Software\Microsoft\Windows\CurrentVersion\Run  
Add:  
"Userinit" = "C:\Documents and Settings\&lt;user&gt;\Application Data\sdra64.exe"*

התוכנית sdra64.exe משתמשת בהזרקת תהליכים כדי להסתיר את נוכחותה ברשימת התהליכים הפועלים. עם ההפעלה, הוא יזריק קוד ל- winlogon.exe (אם קיימות הרשאת אדמיניסטרציה) או ל- explorer.exe (עבור אנשים שאינם בעלי הרשאת אדמיניסטרציה) ויצא.  
הקוד שהוזרק מדביק תהליכים אחרים כדי לבצע את יכולות גניבת הנתונים שלו.

**פירוט טכני נוזקה (מנגנונים פנימיים)**

כאשר תחילה נדבק המחשב, סוס טוראני נוצר בתיקייה “%windir%\system32\wsnpowem”, וכן נשמרים בה הקבצים “audio.dll” ו”video.dll”. הקבצים האלו נועדו לשמירה על המידע הגנוב של המחשב. כמו כן, גם קובץ הקונפיגורציה שיורד לאחר ההדבקה, גם כן נשמר שם. התיקייה נסתרת בעת יצירתה. לאחר מכן הווירוס מעתיק את עצמו לתיקייה “ %windir%\system32\ntos.exe” ובמקרים מסוימים הווירוס משנה את שמו ל-“oembios.exe” (באותו המיקום). אחרי צעד זה, הווירוס בודק האם קיימים תהליכים רצים במחשב הפעילים עם חומת האש. אם אין, הוא יצור קובץ רגיסטר בכדי להריץ את הנוזקה בעת עליית המחשב וכמו כן להמשך בהפצתו.

**פירוט טכני מערך הפצה ושליטת ופיקוד בסדרות תקיפה עיקריות**

ה-ZBot מתחיל בגניבת מידע בכך שהוא פותח תקשורת מול שרת מרוחק ומוריד קובץ קונפיגורציה מוצפן. הקובץ מכיל כתובת אליה הטוראני יעלה בהמשך את המידע הגנוב. כמו כן, הוא יוכל להוריד עדכוני גרסה לעצמו וכן קובץ קונפיגורציה מחודש. הקובץ יכיל רשימה של אתרים אותם הטוראני יסמן לגניבת המידע.  
ברגע שקובץ הקונפיגורציה ירד, כל מידע אישי המקושר לבנק יעבור. אם הקורבן יכניס מידע אודות החשבון שלו באתר אונליין, הטוראני יאסוף את המידע ויעלה אותו לשרת המוגדר בקובץ הקונפיגורציה. כדי לאסוף עוד מידע, כותב הנוזקה יוכל להוסיף עוד שדות לאיסוף, אותם שדות אשר יכנסו לאתר המתחזה.  
ZBot מסוגלים אפילו בהצגת גרסה מזויפת של אתר לקורבן. קורבנות שמנסים לגלוש לאתרים ספציפיים יגלו שינויים מסוימים באתר הנוצרו ע"י השרת שנשלח בידי התוקף, להבדיל מאתר תקין משרת לגיטימי. שוב נזכיר כי האינפורמציה מועברת לתוקף.  
Keylogging, גניבת מידע מהclipboard וצילומי מסך של הdesktop הם גם חלק מארסנל הZBot. הטוראניים גונבים מידע מאובטח מהאחסון, כמו כן תעודות (סרטיפיקייטס) ששמורות במערכת הנגועה. שמות משתמש וסיסמאות לפרוטוקולי POP3 ו-FTP גם כן נגנבים.

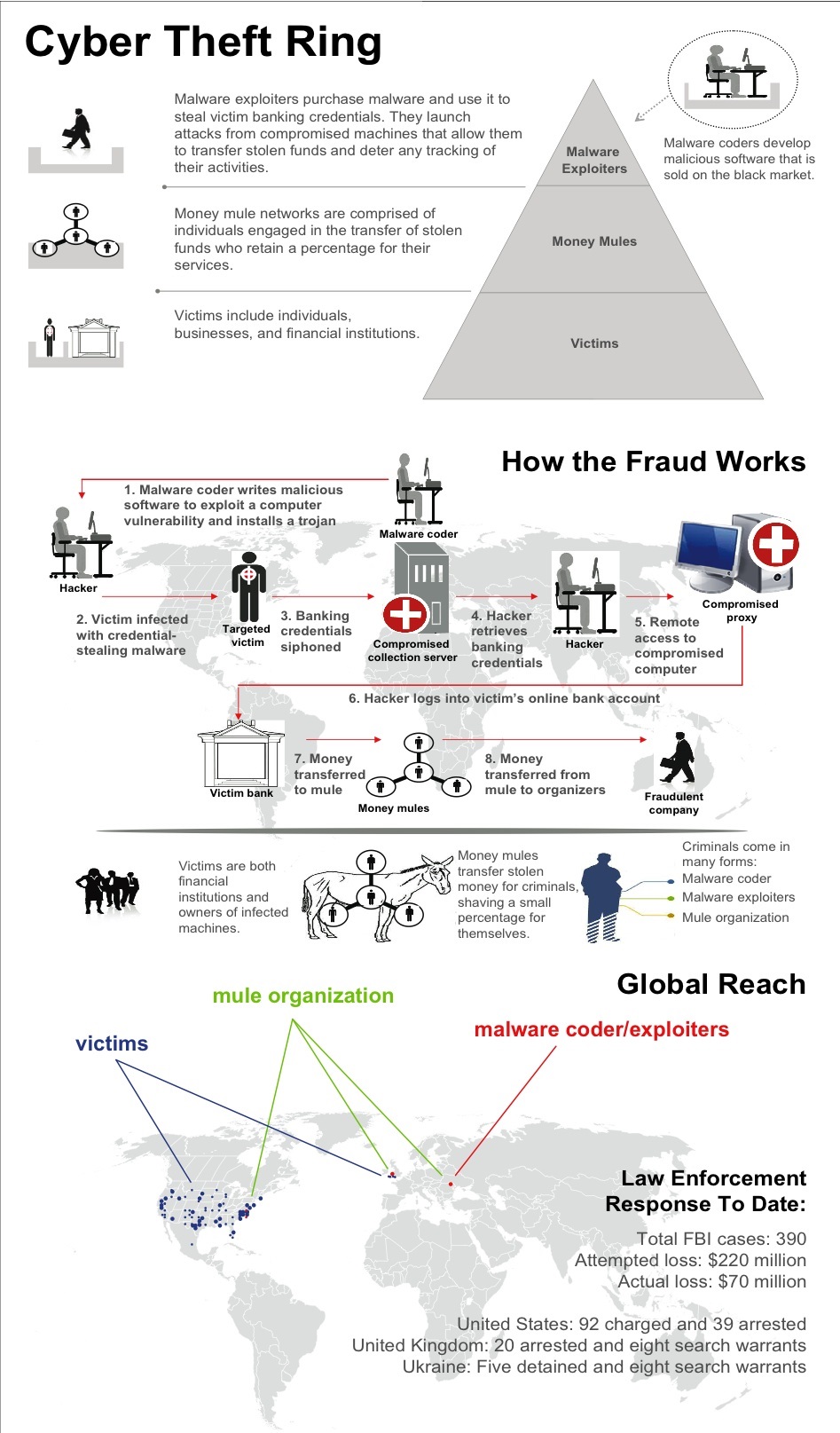
הדרכים הנפוצות ביותר שזאוס מופץ

**Drive-by-downloads**: מפעילי זאוס מאתרים אתרים לגיטימיים, וממנפים את פרצות הדפדפן ומערכת ההפעלה כדי להתקין את התוכנה הזדונית של זאוס כאשר משתמשים ניגשים לאתר.

**הודעות ספאם**: זאוס מתפשט באמצעות דוא"ל 'פישינג' וקמפיינים זדוניים ברשתות חברתיות. מכיוון שהתוכנה הזדונית מסוגלת להשיג גישה בלתי חוקית ל- credentialsשל המשתמש, ניתן להשתמש בה בכדי לחדור לחשבונות מדיה חברתית ולהשתמש בהם לפרסום הודעות פישינג. זה אחד הגורמים שאפשרו לזאוס להתפשט במהירות ולהדביק מיליוני מכשירים ברחבי העולם.

מקרה מפורסם שהתרחש בארצות הברית בשנת 2012, בו השתמשו התוקפים בתוכנה הזדונית של ZeuS. התוקפים הגדירו מספר יעדים בארצות שונות ביניהם: איטליה, הולנד, ספרד, גרמניה ועוד. התוקפים עשו שימוש בעזרת התאמה אישית של תוכנת הריגול ZeuS למובייל, דבר שהוביל ליצירת Zitmo Trojan, המבוסס על ZeuS.  
תוכנה זו נועדה בכדי לעקוף את שלב ה- two-factor authentication(האימות הדו-שלבי), התוכנה מיירטת את מספר האימות (TAN) שהבנקים שולחים למכשיר הנייד של הלקוח באמצעות SMS. קוד זה נועד בעדי לאמת את העברת הכסף מחשבון לחשבון.  
ברגע שלקוח נכנס לחשבון הבנק שלו, אותה נוזקה מזריקה קוד “JavaScript” לחשבון המשתמש.  
בעצם, הקטע קוד הזדוני מודיע למשתמש על "שדרוג אבטחה" ומנחה אותו כיצד לפעול.  
דף שדרוג האבטחה מבקש מהמשתמש לציין באיזו מערכת הפעלה סלולרית הטלפון החכם שלו משתמש - אנדרואיד, בלקברי, iOS (אייפון), סימביאן (נוקיה) או אחרת - כמו גם את מספר הטלפון הנייד שלהם. מידע זה מועבר לאחר מכן ל-“Drop Zone”, המהווה תיקיה הניתנת לצריבה ציבורית בשרת אינטרנט. שם הם מאחסנים מידע על המחשב האישי של כל לקוח בנק נגוע, כולל מספרי חשבון, אישורי כניסה, וסיסמאות חד פעמיות.  
לאחר מכן נשלח SMS אישור מזויף לסמארטפון של המשתמש.  
ה-SMS מכוון את הלקוח להשלים את שדרוג האבטחה על ידי לחיצה על הקישור המצורף. פעולה זו מורידה קובץ למכשיר הנייד של הלקוח עם הגרסה המתאימה והמעודכנת של הנוזקה.  
מכאן ואילך, בכל עת שמשתמשים במחשב האישי בכניסה לאתר הפיננסי הממוקד, עשויות להתקיים התקפות אוטומטיות. כאשר התוכנה הזדונית במחשב האישי מתחילה העברות, והתוכנה הזדונית בסמארטפון מיירטת כל TAN שנשלח על ידי הבנק, ומאשרת אוטומטית את עסקה, ובכך מעבירה את הכסף לחשבונות אחרים.   
במהלך מתקפות אלה, הצליחו התוקפים לגנוב כ-47 מיליון דולר מלמעלה מ-30 אלף לקוחות ברחבי אירופה.





**פרוט כללי וטכני ביחס לקבוצה מאחורי הנוזקה**

במהלך חקירה של ה-FBI פוצחה תעלומת הזהות של העומדים מאחורי הנוזקה ZeuS בראשה עומד אדם בשם Evgeniy Mikhailovich Bogachev, ואף הוצע פרס כספי נכבד למי שיוביל למעצרו (3 מיליון דולר).  
יבגני הידוע בכינויו "Slavik" העומד בראש חבורה הנקראת "צוות ג'אבר זאוס" והכילה 9 אנשים. אחת ממטרותיהם הייתה למכור את הטכנולוגיה לגורמי פשיעה בתמורה לאלפי דולרים.



**בתמציתיות פרוט טכני קצר על ה-CVE ו/או החולשות עליהם מתבססת הנוזקה**

CVE- 2011-3402

שימוש במנוע הפירסור של הפונט בקובץ win32k.sys במצב קרנל בדרייבים ב-Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, R2 SP1, Windows 7 Gold, SP1 מאפשרים תקיפה מרחוק דרך מסמכי Word או אתרי אינטרנט.

CVE-2010-0188

Abode reader בגרסאות מסוימות, מאפשר התקפה ע"י קריסת אפליקציה.

CVE-2012-4681

שימוש ב-Java SE 7 update 6 ומוקדם יותר, מאפשר הרצת קוד זדוני העובר את ה-SecurityManager ויוצר אקספשן מכוון מראש.

CVE-2012-5076

שימוש בJRE שב-Java SE 7 Update 7 כדי לתקוף אלמנטים הקשורים ל-JAX-WS.

**ללא קשר לנוזקה שנבחרה, לבחור מנגנון טכני שנוזקות משתמשות בו ולאתר מאמרים שמתארים את המנגנון**

המנגנון הנבחר הוא Keylogging – שיטה לזיהוי ורישום מקשים אשר נלחצים ע"י הקורבן.

* <https://en.wikipedia.org/wiki/Keystroke_logging>
* <https://enterprise.comodo.com/what-is-a-keylogger.php>
* <https://www.malwarebytes.com/keylogger>

**רשימת מקורות ומאמרים בהם השתמשנו**

* <https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree>
* <https://www.secureworks.com/research/zeus>
* <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/16/the-zeus-zbot-and-kneber-connection>
* <https://www.f-secure.com/v-descs/trojan-spy_w32_zbot.shtml>
* <https://securelist.com/zeus-on-the-hunt/36289/>
* <https://usa.kaspersky.com/resource-center/threats/zeus-virus>
* <https://en.wikipedia.org/wiki/Zeus_(malware)>
* <https://www.fbi.gov/news/stories/gameover-zeus-botnet-disrupted>
* [https://www.cynet.com/network-attacks/zeus-malware-variants-methods-and-history](https://www.cynet.com/network-attacks/zeus-malware-variants-methods-and-history/)
* <https://www.darkreading.com/attacks-and-breaches/zeus-botnet-eurograbber-steals-$47-million/d/d-id/1107673>
* <https://krebsonsecurity.com/2015/02/fbi-3m-bounty-for-zeus-trojan-author>

**מטלה 2: נוזקה משמעותית ומורכבת שקוד המקור שלה דלף**

במטלה זו בחרנו לעסוק בנוזקה בשם KINS.

כחלק מחיפוש הנוזקה, השתמשנו במנוע החיפוש גוגל ובמילות מפתח כמו:  
leaked malware sources, leaked malware, malware source code  
במהלך החיפוש נתקלנו במספר נוזקות ובמספר מאמרים:  
**קוד המקור**  
<https://github.com/alexandreborges/malware-1/tree/master/KINS>  
**מאמרים**  
<https://krebsonsecurity.com/tag/kins-trojan>  
[https://threatpost.com/kins-banking-trojan-a-successor-to-citadel/101440](https://threatpost.com/kins-banking-trojan-a-successor-to-citadel/101440/)  
<http://virus-experts.com/kins-banking-trojan>  
<http://securityaffairs.co/wordpress/38372/cyber-crime/kins-malware-builder-leaked.html>  
[http://blogs.rsa.com/is-cybercrime-ready-to-crown-a-new-kins-inth3wild](http://blogs.rsa.com/is-cybercrime-ready-to-crown-a-new-kins-inth3wild/)  
[https://iicybersecurity.wordpress.com/2015/07/07/kins-malware-toolkit-leaked-online](https://iicybersecurity.wordpress.com/2015/07/07/kins-malware-toolkit-leaked-online/)

**באיזה שפות תוכנה פותחה הנוזקה?**

בעיקר C++, אך גם PHP ו-Python.

**האם ניתוח הקוד טרם להבנת הנוזקה? (אופציונאלי)**

ממומחים טוענים כי התוכנה הזדונית הטרויאנית הבנקאית KINS מבוסס באופן מלא על קוד המקור שהודלף ZeuS, וכולל רק תוספות קלות.  
"התוספות הטכניות אמנם מעניינות, אך הן רחוקות מלהיות פורצות דרך", (מייקל סנדיי, מומחה אבטחה ראשי ב- Fox-IT).  
"עם מגוון של מאפיינים סטנדרטיים למדי, ותוספות פשוטות יחסית ל- ZeuS, הסטנדרטיות, כמו דיווח על מידע, אבטחת מוצר מותקן, פלטפורמת התוכנה הזדונית, אינה מביאה שום דבר חדש באמת.   
עם זאת, ישנם תכונות מסוימות של תוכנה זדונית זו, שאינן מכוונות לפונקציונליות של המשתמש בה, אלא במטרה לסבך את ניתוח התוכנית.

**האם ניתוח הקוד תרם לזיהוי היוצרים שלה ?**

לא, טרם זוהה יוצר הנוזקה.

**האם יש הערכה להיקף ההשקעה בפיתוח התוכנה ?**

בהתבסס על מומחים שניתחו את התוכנה מדובר בקוד שמבוסס על קוד קיים של ZeuS ורק עם תוספות קלות בלבד, מה שמרמז על השקעה לא רבה ביחס לנוזקות אחרות מורכבות.

**איזה גרסה דלפה ?**

KINS 2.0.0.0.

**מאיזה תאריך הפרסום ולאיזה גרסאות של התוכנה הוא מתייחס ?**

פורסם ב-2015, מתייחס לגרסה 1.0.2.0 של התוכנה.

**מהן הפעילויות הנוספות שמיוחסות לקבוצה או לגוף שפיתחו אותה?**

הזהות של מפתח התוכנה טרם ידועה אך:  
ארכיטקטורת KINS דומה לארכיטקטורה שקיים ב-ZeuS/SpyEye עם תוספות של DLL ופלאגינים.  
KINS תואם להזרקות ווב של זאוס, בדומה ל-SpyEye  
סוס טרויאני של KINS מגיע עם התוסף Anti-Rapport שהופיע גם ב-SpyEye  
KINS יעבוד עם RDP (בדומה ל-SpyEye)  
סוס טרויאני של KINS אינו דורש בקיאות טכנית, בדומה לזאוס.  
פרט מעניין נוסף, משתמשים אישיים במדינות ברית המועצות לא יידבקו בנוזקה, דבר זה נראה לראשונה בנוזקה בשם "Citadel" בינואר 2012.  
התפשט באמצעות exploit packs פופולריות כגון “Neutrino” - באמצעות אחת החבילות המתוחכמות ביותר שיש.  
KINS ידביק בקלות מכונות שמריצות מערכות הפעלה Win8 ו-x64 סיביות.  
בעקבות כל הנתונים, ניתן להסיק שהזהות מאחורי המפעיל הינה מברית המועצות, שכן הנוזקה לא תוקפת מחשבים אזרחיים של תושבי ברית המועצות.  
ככל הנראה המפתח של KINS הוא תלמיד נאמן של אבותיו (כדוגמת ZeuS), נוקט בשיטות העבודה המומלצות שלהם ומיישם זאת על תוכנת הנוזקה שלו.