Dear Jonathan,

The following is a preliminary written description of the process we discussed the other day. It is a first draft, and was written to give you something written to refer to when you consult with your colleagues. Unfortunately, it is very unpolished, and also incomplete. Nevertheless, I hope that together with our conversation, this document will give you enough information to decide whether or not this process ("Helena") is "patentable", and if so, what steps need to be taken to reach that end.
Again, I lack the words to describe the appreciation and gratitude I feel. I know you are a very busy man, and I value highly the time you are sparing for me.

Thanks a million
And Shavua Tov

Benny
054-8040040
bhochster@gmail.com

Helena

Contents

1. Short Description

A method (process) for protecting computer files from being manipulated or harvested by background unauthorized malware (such as Trojan horses and similar).

2. Method Summary

1) Software implementing this process is installed on the computer or (in case of a computer network) all computers on the domain.
2) Any file that needs to be protected is flagged through the software.
3) The software continuously monitors file system activity through memory commands.
4) Once the flagged file is called to memory the software intercepts the file, not allowing it to be loaded to local memory before the user authorizes the process.
5) The user is notified on screen that "process X is attempting to access the flagged file". The user than has a choice between either allowing process to access the file or declining it.
6) If the process was invoked intentialy by the user he will allow it (i.e. he started "word" in order to edit the file). But if the process is not recognized by the user, or invoked by some background program, the user can decline. By doing so, the system will immediately terminate the suspicious process, and take any further needed measures to handle the situation (for example, notify sys admin)?

As a result, even if the malware passed through both the antivirus/antimalware and the firewall (usually in cases of target-specific-designed Trojan horse), it will be unable to manipulate or harvest the critical company files.

The following paragraph pretty much says the same as the above, but it is written in a "non algorithmic" manner, and without direct reference to any specific "software". I am not sure, but I think this might matter in the context of patenting the process:
The proposed system secures computer files from hidden and/or background processes by preventing any manipulation of the flagged files without the user's manual confirmation. This is done by continuous monitoring of the computers internal memory for attempts to access or manipulate flagged files. Once such an attempt is detected the user is clearly notified and the attempting process is halted until the user confirms the process to be initiated by him, or otherwise legitimate process.

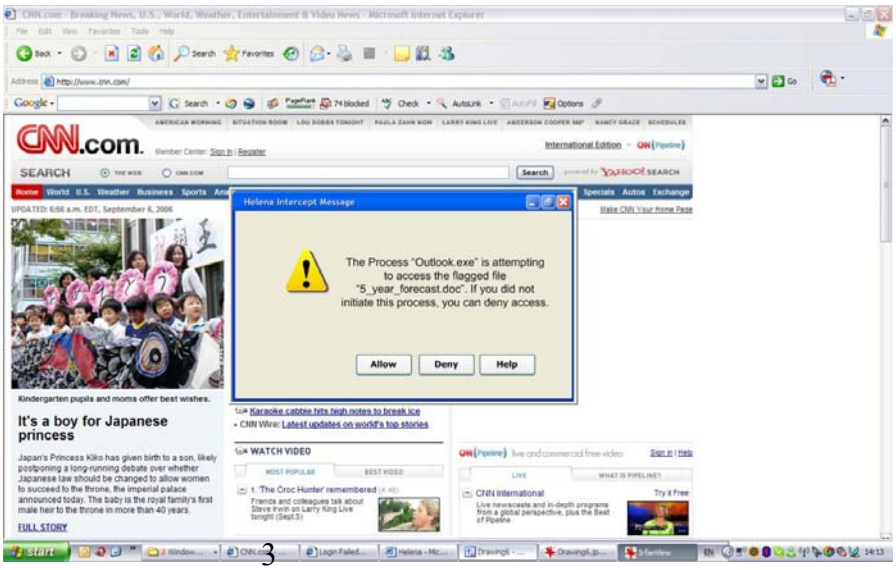


Figure 1: *An alert of a background process calling a protected file generated by software based on this patent.*

3. Background

Up to date, there are 2 major strategies employed to secure sensitive data.

3.1 AntiVirus/AntiMalware

The first are known as "AntiVirus" or "AntiMalware". These programs are designed to monitor the system, and alert – and then fix – the existence of threats in the system. Essentially, all of these programs are based on comparing every program, registry key changes, DLLs etc. to a list made by provider of the service. A provider of such a service will typically monitor internet activity throughout the web, identify malicious software or processes, and than update the client installed on the user's system. Once updated, the client can detect the existence of this malicious code (and sometimes its variants), and take action according to the threat to eliminate the risk.
When this works well, it is a very good technique for handling widely spread malware. It insures that once the malicious code is detected by the service provider, the client antivirus will stop it from penetrating the user's system, and if already penetrated, to eliminate it.
But, the anti malware provides little or no protection from a specific-target-designed malicious program. Unlike most malware, designed to spread to as many computers possible, in order to cause damage or harvest data, sometime (especially for espionage), a malicious peace of software would be written specifically for the system it targets. It will not attempt to multiply or spread beyond the targeted computer or network. (Example: a program designed by competition to corrupt the data on the main server of a big company. This software will not spread, and will never be identified by the antivirus service provider. Hence, the client installed on the computers of the target's computer will not know to consider it as a threat, leaving the entire system exposed.).

3.2 Firewalls

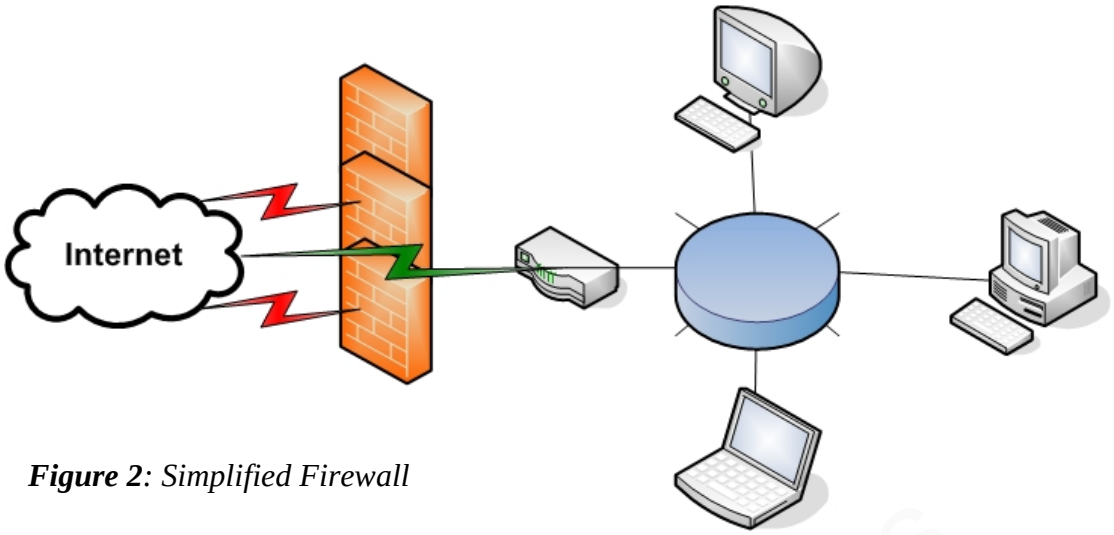


***Figure 2**: Simplified Firewall*

The second is known as a "firewall". Firewalls monitor the systems network connections. There are many different types of firewalls, intending to control the incoming and outgoing communication.
(a) If the firewall identifies an attack from the outside it will stop it before reaching the protected system.
(b) It will also allow the user to allow or deny access to the outside from unauthorized programs
The most important weakness of firewalls is "Trojan horses". Trojan horses coming from the outside via the network (for example, when visiting a malicious internet website, or through the email), might very well be stopped by the firewall, but if the malware is installed BEHIND the firewall (for example, an employee loading a disc he received to his computer, unknowingly releasing the malware hidden on the CD), the firewall will be helpless against it.
Similarly, the firewall would typically be able to stop the malware from accessing the internet, but a smart Trojan horse would not try that. Instead it will use an authorized program to send out the discrete data (example: the firewall probably already knows that the user is authorized to send out emails using the mail client. The Trojan would than send the secret files through email as attachments, leaving the firewall clueless.)

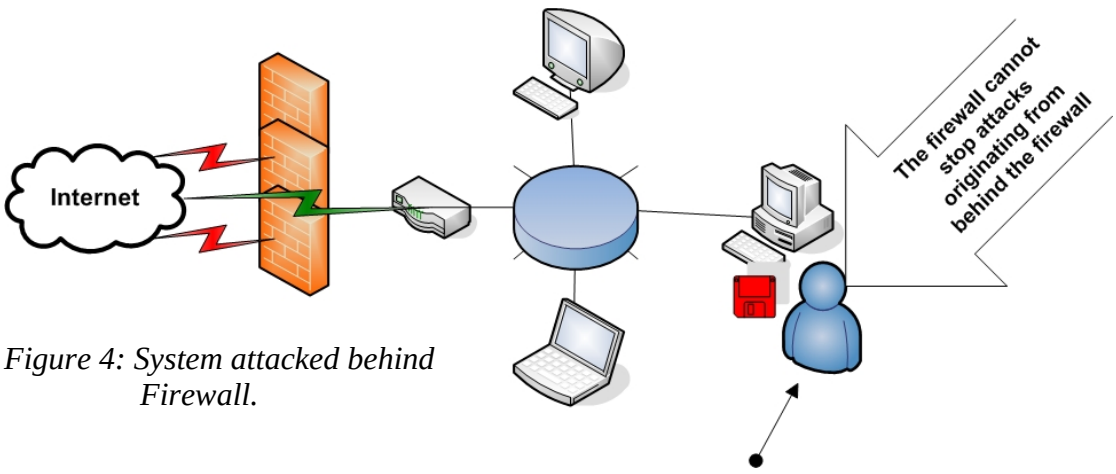


Figure 4: System attacked behind Firewall.

4. The Helena Method

The Helena method is designed to secure critical files even if other solution fail or fall short. In other words, this process will allow for security of the files AFTER the malware overcame the Antivirus and or firewall, and is has already infected the system.
This is done by means of software employing the Helena Approach. The software is installed on all computers on the system (This could mean one personal computer or a large network of computers). Every critical or secret document is flagged in the software.

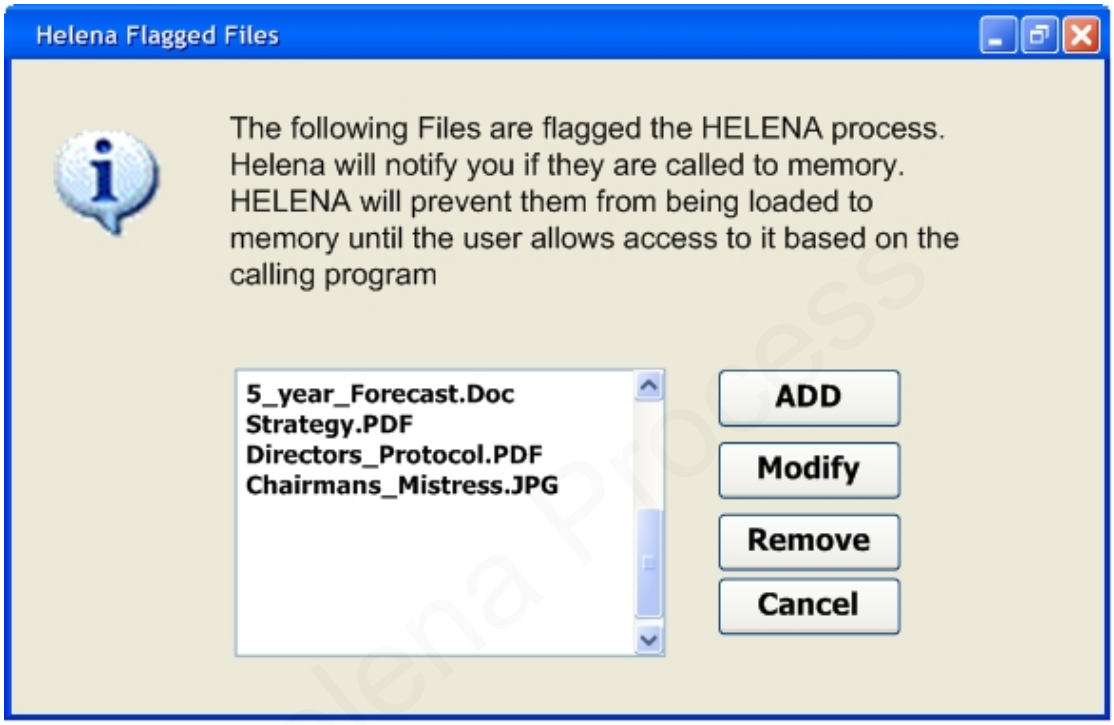
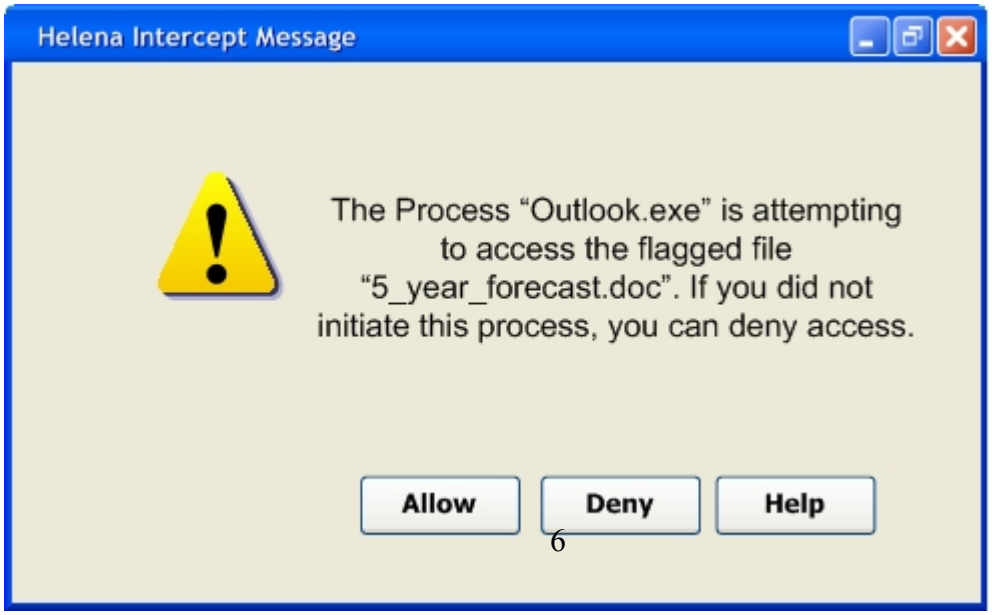


***Figure 5**: Helena Flagged Files*

The software will continuously monitor the computer's memory. Once a flagged file is called to memory by the file system, the software will identify the corresponding process or program, stop the file from being loaded to memory, notify the user onscreen, and ask if to allow the process to proceed or not.



If the user has initiated the process (in the figure above for example, the user is sending the file as an attachment with "Outlook"), he can choose "Allow" and continue.
But if this was not initiated by the user (for example, the alert described in figure X pops up while the user is playing solitaire), that means that this is a result of a process invoked by a background program, possibly with malicious intent.
In this case the user can choose "Deny". This will result in (a) immediately terminating the process. (b) Securing the document immediately and (c) alert the system administrator for further investigation.

4.1 AntiMalware vs. FireWall vs. Helena

An Anti Malware monitors PROCESSES and PROGRAMS, detecting malicious ones. Once detected it would protect the system by means of deleting or quarantining. A malware undetected will be free to cause the damage or steel data from the system. This would usually be the case with non-spreading target-specific malware.

Firewalls, deal with what comes in and what leaves the system. A firewall is helpless when the malware enters the system from within (example – Trojan horse on CD). Moreover, if the malware uses a platform authorized by the user to access outside the network, it will be able to send any file to a remote site as long as that site is not flagged.

Helena monitors FILESYSTEM ACTIVITY and not processes. A malware residing in the system cannot access Helena protected files without the real-time confirmation of the user. Hence, if the process is suspected as malicious, the user will not confirm the access to the file keeping it secure. As a byproduct, Helena in such a scenario, will in fact detect the existence of potential threats undetected by other methods.

5. Scenario Description

Victim LTD is under attack. Their Competition, Evil LTD is after it's forecast. In order to get this data, Evil LTD designs a small software (called "HomonHarosho.exe") to send all files from Victim's computers to an FTP server controlled by Evil. In order to get around Victim's firewall they put it on a CD that also contains the movie "StarTrek 77". They know that Victim's employee, Joe, loves StarTrek, and will be glad to receive it for free. When Joe watches the movie on the company's computer, HomonHarosho.exe installs itself on Joe's computer without Joe's knowledge.
The antivirus installed on this computer checks HomonHarosho.exe against the updated virus dictionary, but since there is no reference to it, and it does not demonstrate typical viral behaviour, the AV does nothing and does not identify HomonHarosho.exe as a threat.

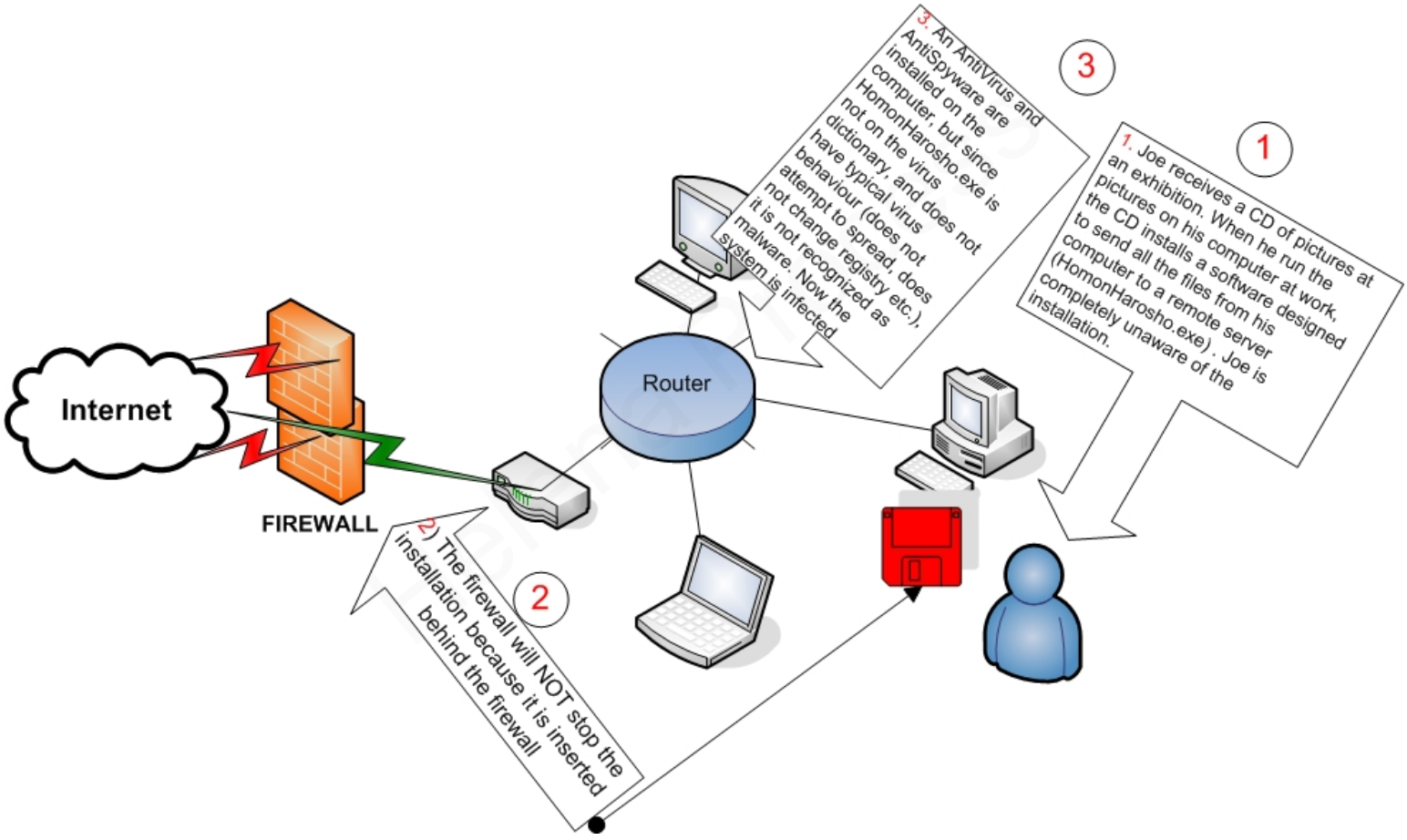
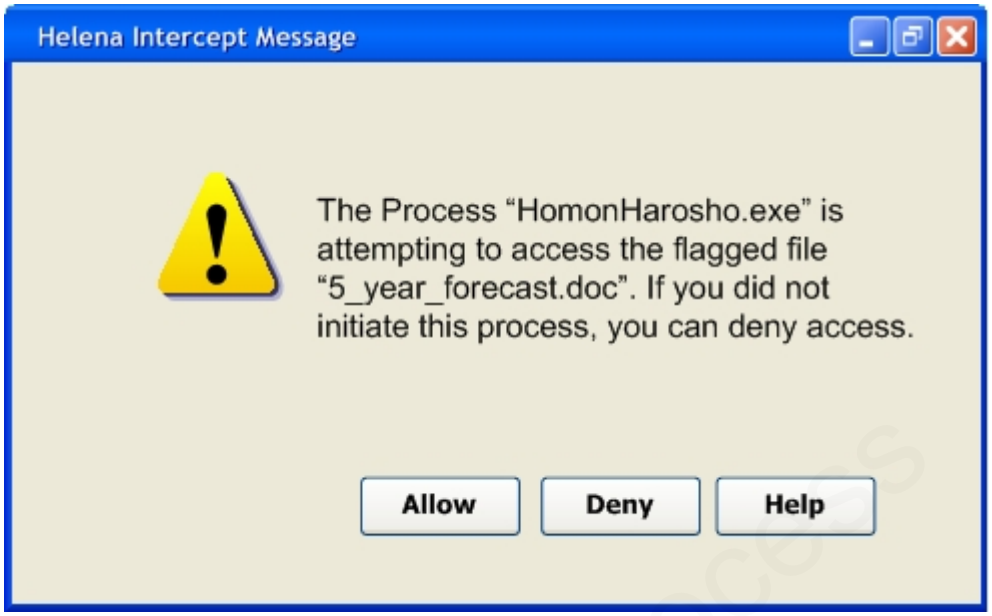


***Figure 7**: The Trojan horse "HomonHarosho.exe" bypasses firewall and antimalware, and infects the computer.*

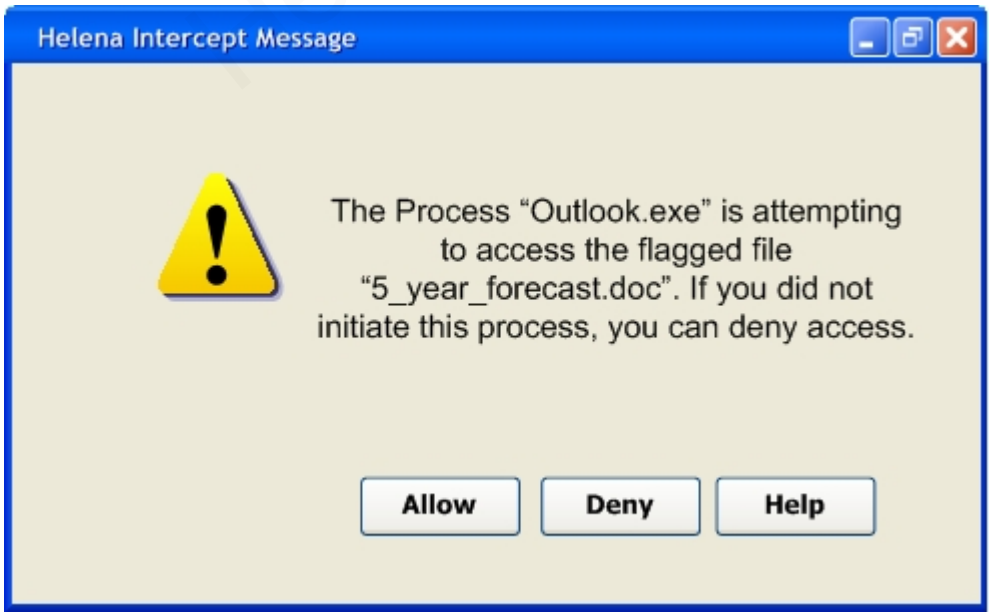
Now the Trojan starts sending files to Evil's remote server. This is done in the background, without Joe knowing. One of the files sent happens to be "5_year_forecast.Doc". This is exactly the info Evil LTD needed to crush Victim LTD….

If Joe would have used Helena, when HomonHarosho.exe would attempt to access a critical file such as "5_year_forecast.Doc" (which would have been flagged to Helena earlier since it is so important), HomonHarosho.exe would not get access to the file. Instead the process would have halted, and Joe would have received a warning message on the screen :



This would appear even in the middle of an exciting solitaire game. Since Joe did not initiate this program he will suspect this process to be malicious, and deny access to the flagged file. This could save the company, not to mention his job.

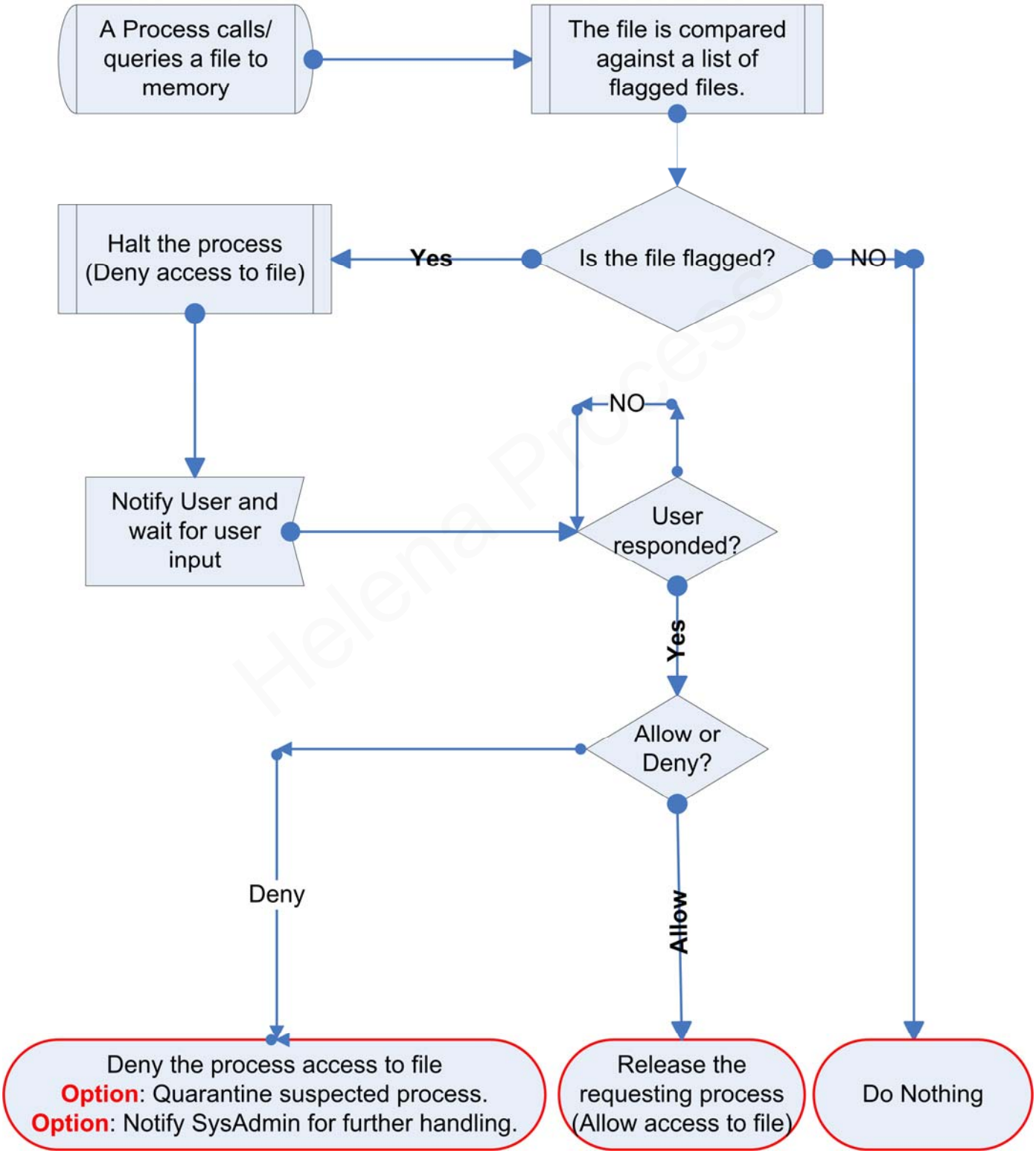
Since Helena does not attempt to "know" when the process is legitimate and when it's not, this alert will come up also when Joe himself tries to access the flagged file. For example, if Joe makes changes to the file, and wants to send it to his colleague for review. Helena will detect this activity halt the process and notify Joe:



Of course, since Joe himself invoked the email client (outlook.exe) he will choose allow and continue working as usual.

Helena Process Streamlined

Helena Has a list of protected ("flagged") files (or file characteristics) as defined by the computer's administrator. The memory is continuously monitored for any filesystem requests



Appendix 1: Some background about the recent Israel Trojan Horse Attack
(Web Pages)

1. **source: http://www.ynet.co.il/articles/0,7340,L-3091872,00.html**

יום הכיפורים של אבטחת המידע

פרשת הסוס הטרויאני חושפת את הבטן הרכה של ארגונים רבים בישראל, המתבססים על מערכות מיחשוב. קשה עד בלתי אפשרי להתגונן מפני סוסים טרויאנים, מספר האיומים גדל כל הזמן והסכנה הגדולה ביותר היא מצד הגורם האנושי
גל מור

פרשיית הסוס הטרויאני עשויה להירשם כקו פרשת המים של תחום אבטחת המידע הממוחשב. גם אם אומדן הנזקים הראשוני יגלה כי היו מקרים חמורים יותר, החקירה האחרונה חסרת תקדים בהיקפה, והיא חושפת את הבטן הרכה של ארגונים רבים בישראל, המתבססים על מערכות מיחשוב. "הפרסום גורם לתהייה כמה מקרים כאלה לא מדווחים ועד כמה חשוף המגזר העסקי", אומר דורון שקמוני, מנכ"ל חברת האבטחה ForeScout ישראל.

עוד בפרשת הסוס הטרויאני:

- **פרשת הסוס הטרויאני - סיקור נרחב**
- **הותר לפרסום: פרשת ריגול במחשבי החברות הגדולות במשק**
- **המזמינים: מפלאפון ועד יס, אלו החברות החשודות**
- **החוקרים: אלה החוקרים הפרטיים המעורבים בפרשה**
- **אמנון ז'קונט ל-ynet: "הסיוט נגמר"**
- **"שימוש בסוס טרויאני אינו חוקי"**
- **"מודיעין עסקי הוא חלק מהחיים במשרדי הפרסום"**
- **תדהמה בספורט: נעצר סגן נשיא מכבי חיפה**

"אין לכם פרטיות בכלל - תתגברו על זה", אמר ב-1999 סקוט מק'ינלי, מנכ"ל סאן מיקרוסיסטמס, וקומם עליו את כל ארגוני הפרטיות. מק'ינלי התכוון לכך שצרכנים שיירצו ליהנות מהפירות של חברת המידע, יתבקשו לוותר על זכותם לפרטיות. זאת, בניגוד לתאגידים שיוכלו להרשות לעצמם להשקיע הון במערכות אבטחה משוכללות שישמרו על סודותיהם קרוב לחזה.

חשופים בצריח

מחקר של "פורסטר" מחודש אפריל גילה כי 47 אחוז מהגולשים לא משתמשים בתוכנות אנטי ריגול. עם זאת, הפרשה האחרונה מרמזת על כך כי גם ארגונים, שלעתים עלולים להינזק הרבה יותר מחשיפת מידע סודי, אינם מודעים כי הם חשופים לגניבת מידע במגוון דרכים שאינן בהכרח מתוחכמות במיוחד.

בעוד ארגונים וחברות מרחיבים בהדרגה את כמות המידע הזמינה ברשת הארגונית, נפערים חורים בלתי נראים באבטחת המידע ומזמינים פורצים להיכנס. בשנים האחרונות האיום הגדול אינו עוד התקפות בלתי מזיקות של נערים פוחזים על אתר האינטרנט של הארגון אלא ריגול עסקי ממוחשב.

הכשל: בודקים את התקשורת הנכנסת לארגון, ולא את היוצאת

שקמוני סבור כי את "האשם" לא ניתן רק לתלות בחוסר הקפדה על נהלי אבטחת מידע אלא גם בכשל מובנה בתורת אבטחת המידע. "אני משוכנע שחלק מהחברות שסבלו מהסוס הטרויאני קבעו נהלי אבטחת מידע, שלא נשמרו במקרה האחרון, אך הבעיה האקוטית היא סוסים טרויאניים, אשר לא בכל המקרים ניתן להתגונן מפניהם. בקהילת אבטחת המידע מזכירים קודים זדוניים כאלה כאיום המרכזי בשנים האחרונות על רשתות ארגוניות.

"אמנם, תוכנות האנטי וירוס יודעות להגן על המחשב מפני חלק מהסוסים הטרויאניים, אשר החתימה שלהם מוכרת לחברות האבטחה, ובשנים האחרונות נכנסו לשימוש גם תוכנות לאיתור חדירות (IDS), אך אם תוכנת סוס טרויאני נכתבת מהיסוד במטרה לחדור לארגון מסוים - קשה עד בלתי אפשרי לעצור אותה".

הגבול בין האינטרנט לארגון מיטשטש

הקונספציה שנכשלה היא התפישה הקובעת גבולות ברורים בין הרשת הארגונית לאינטרנט ומתמקדת בתקשורת הנכנסת לארגון מבלי להקדיש תשומת לב שווה לתקשורת היוצאת מהארגון.

"הגבול בין הארגון לאינטרנט קשה מאוד להגנה ואינו עשוי מקשה אחת", אומר שקמוני, "קוד זדוני עשוי לחדור לארגון דרך קישורי VPN (המשמשים עובדים כדי להתחבר למקום העבודה מהבית), כוננ Flash ועוד. לפיירוול יש ערך אך הוא בוודאי לא חוסם הכל. הלקח החשוב לכל הארגונים הוא כי חשוב לנטר את תעבורת המידע היוצאת מהארגון".

האינטרנט האלחוטי, שחודר בשנים האחרונות גם לארגונים, ומאפשר לעובדים להתחבר לרשת הארגונית מכל מקום, תורם אף הוא לריבוי איומי האבטחה.

בעיה נוספת היא החשיפה של הארגון לפרצות דרך חיבורי VPN מאובטחים. למרות השימוש בחיבור מאובטח, הסכנה הגדולה אורבת מכשלים באבטחת המחשב הביתי של העובד. ברגע שפועל במחשב keylogger או תוכנת שליטה אחרת, העובד שמתחבר לרשת הארגונית מביתו מסייע לפורץ להיכנס הפורץ בעזרת שירותיו הטובים. לעתים ניתן לצמצם את הסיכון באמצעות מערכת הרשאות המצמצמת את יכולתם של מחשבים שמתחברים מרחוק לבצע פעולות מסוימות, אם כי לא בכל הארגונים מקפידים על הרשאות מינימליות. במצב זה, למעשה, כל אדם - עובד זמני, שותף או ספק, הנהנה מגישה לרשת הארגונית עלול לסכן את הארגון.

גם האבטחה הפיזית חשובה נגד ריגול עסקי

לא מדובר רק בגישה 'וירטואלית'. "יש לתת את הדעת לספקים החשופים למידע באמצעות מערכות המחשוב, במקביל לבקר את פעילותם של אלה הנגישים באופן פיזי למידע, כגון אנשי תחזוקה ומנקים, הנכנסים לחברה באופן לגיטימי ומבלי שיעוררו חשד", אומרת מירב ורד, מנהלת תחום מתודולוגיה ותקן 7799 (תקן בינלאומי לניהול אבטחת מידע) בחברת סקיוריטרי, המתמחה באבטחת מידע, "חברות מתחרות רבות עושות שימוש נרחב בספקים מתחזים או אף תוך מתן שוחד לספקים קיימים, על-מנת לקבל מידע חסוי. אסטרטגיה זו פופולרית, זולה ויעילה".

ורד מציינת, כי בעבר, תורות אבטחת המידע נטו להתמקד בהיבטי המחשוב והתקשורת בלבד, אך כיום, בעקבות סיכוני האבטחה ההולכים ומתרחבים, תורות האבטחה מתמקדות בראייה מתודולוגית כלל-ארגונית, המתייחסות למעגלי אבטחה נוספים, בהם אבטחה פיזית, בדיקת מהימנות עובדים, ואבטחת מידע בקרב ממשקים עסקיים.

"המידע הוא הנכס החשוב ביותר בארגון", היא אומרת, "בעולם המודרני משקיעות חברות משאבים רבים במגמה להביא לאבטחה אופטימלית של נכס זה. אבטחה לקויה של המידע עלולה להביא לפגיעה קשה בכושרה העסקי של חברה, ברווחיה, תפעולה או תדמיתה".

מה ניתן לעשות ברמה הטכנולוגית?

שקמוני מציין, כי בשנים האחרונות נכנסו לשימוש מספר טכנולוגיות נלוות המיועדות לצמצם את הסיכונים, בהן מערכות ניטור והגנה למניעת חדירות (System Intrusion Detection, ובקיצור, IDS), המתריעות במקרים של תעבורת מידע מעוררת חשד. סוג אחר של תוכנות מיועד לפקח על חיבור של אמצעי מדיה נתיקים כמו כוננ Flash ותקליטורים, אך

מדובר בתחום שנמצא עדיין בחיתוליו".

אנשים הם החוליה החלשה

למרות זאת, שקמוני מסכים כי במקרים מסוימים הטכנולוגיה לא תוכל לעזור כלל. "אין הגנה טכנולוגית נגד אנשים החושפים את הארגון מבפנים - אם במתכוון או לא. תוכנה תתקשה מאוד להבדיל בין עובד שממלא בטופס את פרטי כרטיס האשראי שלו - לצורך רכישת מוצר באתר מסחר אלקטרוני לבין תוכנה המשתמשת ביציאה של הדפדפן לאינטרנט כדי לשלוח מידע מסווג.

"צריך להבין כי תוכנה קטנה שחודרת למחשב אחד ברשת הארגונית עלולה לסכן את כל משאבי הארגון. לעתים, קוד שרץ על מחשב של משתמש מסוים עלול להאזין לתעבורה ברשת ולפלס את דרכו למידע סודי, גם אם אותו משתמש אינו מורשה לצפות במידע זה".

"אנשים הם החוליה החלשה בשרשרת אבטחת המידע. יש צורך באכיפת נהלי אבטחה קפדניים כדי למנוע הישנות מקרים כאלה. ההמלצה החשובה ביותר היא בשום פנים ואופן לא להריץ בארגון תוכנה שאינכם בטוחים לחלוטין באמינותה ומוטב לא להריץ תוכנות חיצוניות ללא אישור של מנהל אבטחת המידע ברשת. הבעיה היא שישראלים מסרבים להישמע להוראות".

פתרונות קיצוניים

המודעות לבעיות האבטחה מביאה לכך שחלק מהארגונים חוששים להתחבר לרשתות חיצוניות ללא אמצעי אבטחת מידע נאותים ולכן מעכבים את התחברותם – דבר שפוגע בפעילותם ובעסקיהם.

גישה נוספת דוגלת בצמצום סיכוני האבטחה באמצעות מעבר לשימוש בלקוחות רזים בארגון. על פי התפישה הישנה-חדשה הזו, המחשב של העובד אינו אלא מסוף של שרת מרכזי המשמש להרצת יישומים. אי אפשר להתקין על המחשב

או תקליטורים. "זו תפישה שעשויה לשפר את האבטחה במידה רבה, אך היא Flash כרוכה בשינוי מהותי בהרגלי העבודה של המשתמשים בארגון", אומר שקמוני.