For English version click here

שלום לבית הטכניון

"פשעי סייבר הם האיום הגדול ביותר על כל חברה בעולם".

***ג'יני רומטי** - שימשה בעבר כיו"ר, נשיא ומנכ"ל IBM, והפכה לאישה הראשונה שעומדת בראש החברה.*

1. **קודי QR יכולים לרושש אותך**, מזהיר ה-FBI או בעברית היזהר קוד QR לפניך. כולנו למדנו את התורה (אני מקווה) ויודעים שלא מקישים על קישור חשוד ולא פותחים צרופה במייל חשוד. חשוב להפנים כי לשני אלה יש בן דוד מסוכן באותה מידה.
קודי QR זכו לעדנה בתקופת מגפת הקורונה. מסעדות ועסקים אחרים פרסו אותם במספרים גדולים במהלך השנים האחרונות, במאמץ לייצר יותר אינטראקציות ללא מגע.
ה-FBI מזהיר שגם רמאים אוהבים אותם. פושעי סייבר מנצלים את הטכנולוגיה הזו על ידי:
- הפניית סריקות קוד QR לאתרים זדוניים כדי לגנוב נתונים של הקורבן
-הטמעת תוכנות זדוניות כדי לקבל גישה למכשיר של הקורבן, והפניית תשלומים בצורה זדונית
Ars Technica דיווחה על קודי QR מזויפים שהודבקו על מדחני חניה בערי טקסס, במטרה ליירט תשלומים.
התרמית מתרחשת בדרך כלל באמצעות קוד QR זדוני, על מסך או על דף מודפס. קורבנות סורקים את מה שהם חושבים שהוא קוד לגיטימי, אבל הקוד הזדוני מפנה את הקורבנות לאתר זדוני, אשר מבקש מהם להזין פרטי התחברות ומידע פיננסי.
על המשתמשים לבדוק את כתובת האתר שנוצרת על ידי קוד QR, ולהיזהר מהשימוש בהן באופן כללי, במיוחד לצורך ביצוע תשלומים.
היזהרו מקודי QR כמו עם כתובות URL וצרופות!

2. **סורקי אבטחה ברחבי אירופה קשורים לממשלת סין**.
בכמה מהמקומות הרגישים ביותר בעולם, הרשויות התקינו מכשירי סריקת אבטחה מתוצרת חברה סינית, אשר לאחת הבעלים שלה קשרים עמוקים לצבא סין ולרמות הגבוהות ביותר של המפלגה הקומוניסטית השלטת. הנתונים המעובדים על ידי סורקים אלה רגישים מאוד. אלה נתונים אישיים, נתונים צבאיים ונתוני מטען. אלה יכולים לכלול סודות מסחריים רגישים. החשש נובע מכך שחוקי המודיעין הלאומיים של סין, מחייבים חברות סיניות למסור נתונים המתבקשים על ידי סוכנויות הביטחון של המדינה. אחרים עשויים לומר שסיכון דומה קיים עם ציוד מתוצרת ארה"ב. אכן, חומר למחשבה.
תחשבו טוב מה אתם רוכשים ליישומים השונים!

3. **מאז לידתן של מערכות ההפעלה אנדרואיד ו-iOS**, הטלפונים החכמים התפתחו הרבה מעבר ליכולות של שיחה וטקסט. כעת אלה מכשירים חכמים המסוגלים לבצע משימות שבעבר בוצעו על ידי מחשבים בלבד. אנו משתמשים בהם כדי לצלם תמונות, לשלח ולקבל אימיילים, לתקשר באמצעות פלטפורמות של מדיה חברתית, לעבוד עם ארנקים ואפליקציות בנקאיות... הרשימה עוד ארוכה. כל שפע הנתונים הזה מושך גם גורמים עוינים שרוצים

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

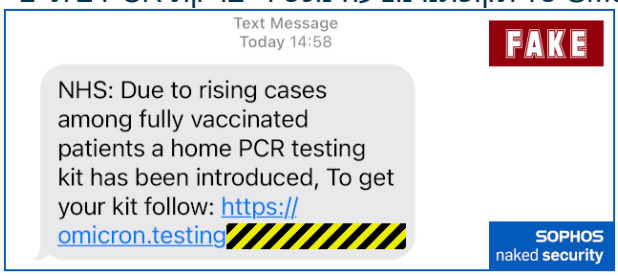
TECHNION
Israel Institute
of Technology

Tel: +972 48294192
glickstein.m@technion.ac.il \ cis.technion.ac.il

להשתמש בהם למטרותיהם – ממכירת הנתונים ברשת החשוכה של האינטרנט ועד לשימוש לצורך ביצוע גניבת זהות והונאה.
השנים האחרונות סיפקו שפע של ראיות לכך שכל טלפון חכם עלול להיפגע על ידי תוכנות זדוניות. כאשר אנדרואיד מחזיקה בחלק הארי של השוק ונחשב לפחות מאובטח מ iOS, אנו נתמקד במערכת ההפעלה הזו ונמנף תובנות של חוקר תוכנות זדוניות של ESET בשם Lukas Stefanko, שיש לו רקורד ארוך של חשיפת איומים המכוונים למשתמשי אנדרואיד.
לקריאת המאמר בשלמותו (מומלץ)

4. **תרמיות COVID** - כפי שאתם בוודאי יודעים, בדיקות PCR, שדורשות כיום עיבוד במעבדה, נחשבות מדויקות יותר מבדיקות אנטיגן בביצוע עצמי. בדיקות PCR מוסיפות זמן עד לקבלת התוצאה. אז, כפי שאתם יכולים לדמיין, לכל מי שיש חובה או אחריות אישית וצריך לצאת לעבודה שלו - שרברבים, חשמלאים, עובדים סיעודיים, צבעים, מורים, מרצים, סטודנטים ועוד עשרות מקצועות אחרים - מכשיר PCR לבדיקת ביתית היכול להפחית את הזמן לקבלת תוצאה מהימנה יהיה שימושי מאוד.

הונאת SMS של תקופתנו מציעה מכשירי בדיקת PCR ביתיים - אל תיפלו בפח, אין כאלה בינתיים!



5. **אני שמח לבשר כי נבדק ואושר TOKEN** של חברת YubiKey לטובת הזדהות חזקה MFA כתחליף (במקרים בהם נדרש) להזדהות באמצעות הטלפון החכם.
המוצר - https://www.yubico.com/ של חברת YUBICO מסדרת YubiKey 5 – שימו לב לחיבורים השונים USB או USBC
קיים ספק ישראלי המייצג את היצרן בישראל – הספק מוגדר ברכש בטכניון.
https://multipoint.co.il/yubikey-5/
ההגדרה פשוטה ומתבצעת ע"י המשתמש הסופי באמצעות "Add Method" במערכת ה 365.

המוצר יכול להתאים בין היתר למצבים הבאים:

א. משגיחי בחינות – יקבלו את ה TOKEN לפני בחינה. ה TOKEN ישודך למחשב/משתמש בחדר מסוים.
ב. למתנגדי הטלפון החכם.
ג. כגיבוי לטלפון חכם שאבד או בתיקון.

החיסרון – אם משאירים את ה TOKEN באופן קבוע במחשב (במיוחד ציבורי) !!!

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION Israel Institute of Technology
Tel: +972 48294192
glickstein.m@technion.ac.il \ cis.technion.ac.il

6. אבטחת סייבר בשנת 2021 – סיכום שנה (קריאת העשרה עם מינוח טכני מועט מאוד)

הסוס הטרויאני הראשון (לא היווני העתיק😊) נשלח על גבי תקליטון למוסדות מחקר ברחבי העולם בשנת 1989 ומאז תוכניות מחשב זדוניות גרמו נזקים של מיליארדי דולרים לצרכנים, לעסקים ולממשלות.

2021 הייתה שנה מאתגרת - ולעתים גם מפחידה - עבור מקצועני אבטחת סייבר עם מגוון של התקפות ששיבשו פעילות עסקית, פגעו בשרשראות אספקה ואף הובילו להשבתות עסקיות. ראינו התקפות מתוחכמות על גורמי ממשל על ידי ישויות בחסות מדינות. ראינו עלייה מובהקת בתוכנות כופר שמשביתה תשתיות ליבה של ארגונים. ראינו פרצות בשרשרת האספקה שמשפיעות על מאות, אם לא אלפי, ארגונים.

להלן 5 מתקפות מובילות של 2021 והלקחים לכולנו.

SOLARWINDS -1

כל אחד צריך לדעת אילו נכסי IT בבעלותו והיכן הם נמצאים, מכיוון שהתקפות יכולות להגיע מכל מקום, כולל משרשרת האספקה. חברת SOLARWINDS היא מהגדולות בעולם בתחום של ניטור תקינות ומצבם של התקני רשת שונים ובכלל זה שרתים, תחנות וכיו"ב. סיפרתי על כך באחד הגיליונות של 2021.

העובדות:

בדצמבר 2020, חברת אבטחת הסייבר FireEye הודיעה שהיא קורבן למתקפה שבה נגנבה ערכת הכלים של Red Team שלהם; מאוחר יותר באותו החודש הודיעה FireEye ל-SolarWinds שתוקפים נכנסו למערכות שלהם דרך דלת אחורית השתולה בעדכון התוכנה של SolarWinds. APT29, שחקן סייבר ברמת מדינה המזוהה עם סוכנויות הביון של רוסיה, ניצל את התוכנה המסחרית של SolarWinds על ידי הטמעת תוכנות זדוניות בעדכון התוכנה אשר אפשר לתוקפים להשתמש בקוד בצורה של סוס טרויאני ולהיכנס לכל מכשיר ומערכת שהוא מוגדר לנטר ולנהל.

<u>לקח שנלמד מ-Solarwinds</u>

התקפות יכולות להגיע מכל מקום, אפילו מהספקים המהימנים ביותר בשרשרת האספקה , כמו SolarWinds. זה נכון במיוחד כאשר אותם ספקים משמשים כמטרה של תוקפים זדוניים מתוחכמים מאוד בחסות מדינה. חשוב מאוד לדעת באילו נכסי IT אתה משתמש והיכן הם נמצאים. הידע על הנכסים שלך, מי הבעלים שלהם ועד כמה הם קריטיים לעסק מאפשר לך להגיב במהירות לסיכונים לנכסים אלה. לגבי התקפת SolarWinds, אם הנפגעים ידעו את משטח ההתקפה שלהם, כולל שרשרת האספקה, אז ברגע שנודע להם על הפרצה הם יכלו לדעת אם הם הושפעו. וזאת בניגוד מוחלט לשעות, לימים, לשבועות שזה עלול לקחת ולקח לארגונים רבים.

<u>האם כל אחד מאיתנו יודע היכן כל הנתונים שלו?</u>

<u>GoogleDrive, SharePoint, DropBox, אחסון מרכזי, עוד.</u>

COLONIAL PIPE -2

העובדות:

בתחילת מאי 2021, קבוצת תוכנות הכופר DarkSide השביתה כ 5,550 מיילים של צינור נפט, ותקעה חביות של בנזין, סולר ודלק סילוני בחופים הדרומיים של ארה"ב. נראה שהאקרים נכנסו דרך ה-VPN של החברה באמצעות סיסמה שנחשפה. הקבוצה מפעילה

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION Israel Institute of Technology
Tel: +972 48294192
glickstein.m@technion.ac.il \ cis.technion.ac.il

את תוכנת הכופר שלה - שנקראת "DarkSide ransomware" וסופקה כשירות ברשת - נגד חברות אמריקאיות ואירופיות במשך חצי שנה לפחות. תוקפים המשתמשים בגרסת תוכנת הכופר של DarkSide מקבלים בדרך כלל גישה ראשונית על ידי ניצול שירותי גישה מרחוק כמו Citrix, Remote Desktop Web (RDWeb), או פרוטוקול שולחן עבודה מרוחק (RDP) ממקור התקפה חיצוני. ברגע שהם משיגים דריסת רגל, הם חופרים עמוק יותר באמצעות תנועה לרוחב הרשת, מוציאים נתונים, ואז מצפינים באמצעות תוכנת כופר כדי לסחוט כסף מהקורבנות שלהם.

לקח שנלמד מצינור קולוניאלי

התקפות מוצלחות של תוכנות כופר הן עסק גדול - אפילו בהתחשב בכך שחלק מכספי הכופר במקרה זה הוחזרו. החזר על ההשקעה ה-ROI לתוקפים של התקפות כופר כמו זו נאמד ב-1,400%. בדרך כלל, תוקפים אלה מבצעים לימוד מקדים, ורק אז, הם ניגשים למטרה דרך סוג כלשהו של שירות גישה מרחוק. הם הולכים לרוחב כדי למצוא ולהצפין נכסים יקרי ערך. המגיפה והעבודה מהבית הקלה מאוד על קבוצות כמו DarkSide למצוא מטרות.

תוקפי כופרה הפכו מתוחכמים למדי בשנה האחרונה, "מפלחים את השוק" ומנהלים קמפיינים בקנה מידה גדול נגד ארגונים קטנים ובינוניים, וקמפיינים ממוקדים יותר נגד ארגונים גדולים או כאלה הנחשבים לתשתיות קריטיות (כמו בתי חולים, ספקי אנרגיה ושירותים אחרים ורשויות ממשל).

בהתחשב בשילוב של עסקים גדולים ודולרים גדולים עבור תוקפים בכופרה, ההגנה הטובה ביותר היא להבטיח שאתה מאבטח שירותים מרוחקים.

חשוב להתחבר מרחוק אך ורק באמצעות ה SSLVPN הטכניוני. בסיום העבודה להתנתק מהרשת ואם מדובר על מחשב שאינו פרטי לסגור את כל החלונות ואם אפשר גם לבצע כיבוי או RESTART.

3- פגיעות של MICROSOFT EXCHANGE (ישנים וחדשים!)

מספר חולשות הופיעו בשרתי Microsoft Exchange בשנת 2021. החולשות רלוונטיות לשרתי 2010, 2013, 2016 או 2019. על פי הדיווחים, הפגיעויות ניצלו במספר הזדמנויות חולשות Zero Day, בהם נעשה שימוש לקבלת גישה לחשבונות דואר אלקטרוני ושתילת תוכנות זדוניות.

כל הפגיעויות שהוזכרו לעיל מאפשרות לתוקף לשתול קובץ בשרת. בעוד שחולשות אלה קיימות כנראה זמן רב, הניצול שלהם זינק במהלך 2021. במהלך מספר ימים מספר הקורבנות הפוטנציאליים עלה מ-30,000 ל-60,000 ויותר ליום.

לקח שנלמד מ-Microsoft Exchange

כפי שניתן לראות, חלק מהחולשות נמצאות במערכות ישנות יותר, ובמקרה של שרתי Exchange 2010 מדובר בגרסה שאינה נתמכת עוד על ידי מיקרוסופט. השיעור הראשון כאן הוא - **אל תשכח את הציוד הישן שלך... כי התוקפים יזכירו לך**. חייבים לפקח באופן רציף על כל משטח ההתקפה החיצוני לאיתור בעיות אבטחה, במיוחד בציוד הישן יותר.

בנוסף, גם אם חברה שדרגה או החליפה מערכות שנמצאות בסיכון, אסור להניח שכל מי שאתה עושה איתו עסקים עשה זאת גם. ייתכן שחברת בת קטנה של אחד מהספקים לא טרחה להחליף שרת ישן שעובד "בסדר גמור". הדבר נכון גם לשותפים. אל תאפשר לאף גורם חיצוני להתחבר אליך ללא פיקוח של צוות ה IT

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION Israel Institute of Technology

Tel: +972 48294192
glickstein.m@technion.ac.il \ cis.technion.ac.il

4 - ACCELLION

חובה לרענן בארגון את מדיניות גילוי המתקפות ולהיות בטוח שכאשר אתה מתמודד עם בעיה (כמו מתקפה), אתה אומר את כל האמת.

העובדות:

Accellion התקשרה עם צד שלישי במרץ 2021 כדי לחקור התקפות על המוצרים הישנים שלה. Accellion, **שהוציאה בשקט תיקון** בדצמבר, לא טרחה לידע את הלקוחות או הרשויות על חומרת הבעיה. המתקפה השתמשה בשילוב של חולשות ZERO DAY כדי לגנוב נתונים שהוצעו לאחר מכן תמורת כופר. התוקפים, החלו להוציא מכתבי סחיטה בחודש ינואר. הקורבנות היו לקוחות ואפילו לקוחות של לקוחות של Accellion, כולל מוסדות פיננסיים ובריאות גדולים, כמו גם מספר אוניברסיטאות וקמעונאים גלובליים.

לקח שנלמד מ Acccelion

אחד הלקחים הגדולים ביותר שנלמדו ממתקפת Accellion הוא זה שאולי אמא שלנו לימדה אותך: "ספר את כל האמת". נושא הדיווח הקשור למתקפות (יחד עם "אל תשכח את הציוד הישן יותר") הוא ש Accelion ניסתה להמעיט בחומרת הבעיות וכתוצאה מכך פגעה בעצמה ובלקוחותיה. ההתקפות המשיכו להופיע חודשים לאחר היוודע החולשה ליצרן, מכיוון שללקוחות לא היה את המידע הנכון לטפל בחולשה.

סדרת אירועים זו משמשת גם כתזכורת שעדיף שיהיו כללי גילוי של חולשות לפני שהמתקפה מתרחשת. חשוב שהגילוי יהיה נאות ומפורט.

נתקלת בחשד לאירוע, אל תהסס ודווח מייד לנאמן האבטחה ביחידתך או ישירות ל CISO.

5 - פריצות לשירותי המים של פלורידה וקליפורניה

העובדות:

בפברואר 2021, עובד מפעל טיהור מים באולדסמר, פלורידה הבחין שמישהו אחר שולט מרחוק במחשב שלו. ככל הנראה, התנהגות זו כשלעצמה לא הייתה מדאיגה כי גישה מרחוק משמשת בדרך כלל לפתרון בעיות IT, אבל מה שהיה מדאיג הוא שהאדם אשר שלט ניסה להעלות את כמות החומר - נתרן הידרוקסיד במים לרמות מסוכנות. למרבה המזל, העובד הצליח לפעול במהירות ולסכל את מה שיכול היה להיות מתקפה מסוכנת ומסכנת חיים.

בינואר 2021 מערכת מים נוספת, הפעם בסן פרנסיסקו, קליפורניה, נפגעה באופן דומה. שוב, לשירות המים ניגשו התוקפים באמצעות חשבון פעיל ב-TeamViewer, תוכנת צד שלישי המאפשרת קישוריות בין מחשבים לגישה מרחוק ותמיכה. התוקף, לאחר שנכנס, המשיך למחוק תוכניות לטיפול במי שתייה. התקיפה התגלתה במהירות - למחרת.

הלקח שנלמד

קבוצת האיומים האחרונה הזו תוכננה על ידי תוקפים כדי לעורר פחד, שכן הם כיוונו לתשתיות קריטיות - מערכות מים. הוסיפו לאלה את השבתת הצינור הקולוניאלי של צינור נפט מרכזי בארה"ב והתקפות תוכנות כופר על בתי חולים ואנו רואים שלא נראה שיש גבול מוסרי או אנושי למה שתוקפים יעשו, ואלו מערכות הם מוכנים להשבית או לפגוע.

חשוב שכולם ימשיכו לשמור על ערנות ולעשות כל שביכולתם כדי למנוע מתוקפים להיכנס למערכות שלהם.

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION Israel Institute of Technology

Tel: +972 48294192
glickstein.m@technion.ac.il \ cis.technion.ac.il

השאלה מהגיליון הקודם

המחשב שלך נדבק זה עתה בתוכנת כופר וההאקר דורש כסף כדי לשחרר אותו. מה אתה עושה?
א - שולח דוא"ל לאיש ה- IT במשרד.
ב - מנסה כמיטב יכולתך להיפטר מהבעיה לפני שמישהו יגלה זאת
ג - משלם את הכופר. אתה צריך את הקבצים שלך בחזרה!
ד - מנתק את המחשב מהרשת.
התשובה הנכונה היא "ד" - זה הדבר הראשון שצריך לעשות. זה מנתק את התוקף מהמחשב שלך. רק לאחר הניתוק ביצוע הטיפול הטכני יכול להתחיל. הסבר בונוס - כיבוי המחשב עשוי להפעיל תהליכים לא רצויים לאחר הפעלה מחדש או מחיקת ראיות שישמשו לתחקור.

שאלה חדשה :

מי אחראי על אבטחת המידע בארגון?
1.המנכ"ל (CEO)
2. המנמ"ר – מנהל מערכות מידע ומחשוב (CIO)
3. כל המשתמשים בארגון
4. ממונה אבטחת המידע (CISO) ונאמני האבטחה ביחידות

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION
Israel Institute
of Technology

Tel: +972 48294192
glickstein.m@technion.ac.il \ cis.technion.ac.il

Dear Technion Family

"Cybercrime is the greatest threat to every company in the world."

Ginni Rommety ***previously served as chairman, president and CEO of IBM, becoming the first woman to head the company.***

1. QR codes can eat your lunch, FBI warns

QR codes are among the few "winners" of the coronavirus pandemic, the joke goes, because restaurants and other businesses have deployed them in far greater numbers over the past few years, in an effort to make more interactions contactless.

We all have learned by now (I hope) and know not to click on suspicious links and not to open an attachment in a suspicious email. It is important to understand that these two have an equally dangerous "friend".

The FBI is warning, however, that scammers love them, too. Cybercriminals are taking advantage of this technology by directing QR code scans to malicious sites to steal victim data, embedding malware to gain access to the victim's device, and redirecting payment for cybercriminal use, the announcement says.

Ars Technica reported on fake QR codes that were stuck on parking meters in Texas cities, with the goal of intercepting payments.

The trickery usually comes through QR codes that have been altered, either onscreen or on a printed page. A victim scans what they think to be a legitimate code but the tampered code directs victims to a malicious site, which prompts them to enter login and financial information, the FBI said.

FBI is warning consumers to double-check any URL generated by a QR code, and to be cautious about using them in general, especially for making payments.

Beware of QR codes as much as with URLs and attachments!

2. Security Scanners Across Europe Tied to China Govt, Military.

At some of the world's most sensitive spots, authorities have installed security screening devices made by a single Chinese company with deep ties to China's military and the highest levels of the ruling Communist Party. The data being processed by these devices is very sensitive. It's personal data, military data, cargo data. It might be trade secrets at stake. Critics fear that under China's national intelligence laws, which require Chinese companies to surrender data requested by state security agencies. Others may say that similar risk exist with US made equipment. Indeed, food for thought.

Always think before a purchase what you buy for specific use cases!

3. With the dawn of the Android and iOS operating systems, smart phones have evolved far beyond their humble call and text features – they now are portable smart devices capable of doing tasks that were previously entrusted to laptops and PCs. We use them to snap pictures, send and receive emails, communicate through social media platforms, for

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION Israel Institute of Technology

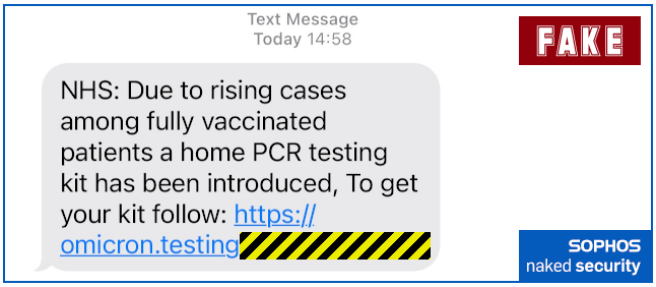
Tel: +972 48294192
glickstein.m@technion.ac.il \ cis.technion.ac.il

wallets and banking apps … the list goes on. All of that wealth of data also attracts threat actors who want to use it to their own ends – from selling it on the dark web to using it to commit identity theft and fraud.

The past few years have provided plenty of evidence that even your trusty mobile device can be compromised by malware. With Android holding the lion's share of the market, we'll focus on this OS and leverage insights from ESET malware researcher Lukas Stefanko, who has a long track record of uncovering threats targeting Android users.

To read the complete article. (Recommended)

4. As you probably know, PCR tests, which currently require processing in a laboratory, are considered more accurate than self-administered lateral flow tests. PCR Tests add time until you get the result. So, as you can imagine, for anyone with accountability who is for example self-employed but who needs to be out and about for their job – plumbers, electricians, care workers, painters and dozens of other professions – a home testing PCR device that could reduce the time to receive a trustworthy result would be very useful.



Coronavirus SMS scam offers home PCR testing devices – don't fall for it, such do not exist yet!

5. **I'm happy to announce that YubiKey's TOKEN** has been tested and approved in favor of strong MFA authentication as an alternative (where required) for smartphone.
The product - https://www.yubico.com/ of the YUBICO company. The solution is the YubiKey 5 series - pay attention to the various USB or USBC connections. There is an Israeli supplier that represents the vendor in Israel - the supplier is set up in procurement at the Technion.
https://multipoint.co.il/yubikey-5/
The settings are simple and done by the end user using the "Add Method " in 365.
The product is useful in the following situations:
A. Exam supervisors - will receive the TOKEN before the exam. The TOKEN will be matched to a computer / user in a specific room.
B. For those who do not use a smartphones.
C. As a backup to a lost smartphone or in repair.

The downside - if you leave the TOKEN permanently on the computer (especially public)!!!

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION
Israel Institute of Technology

Tel: +972 48294192
glickstein.m@technion.ac.il \ cis.technion.ac.il

6. CYBERSECURITY IN 2021 – SUMMERY (READING ENRICHMENT WITH VERY LITTLE TECHNICAL TERMINOLOGY)

The first Trojan horse (Not the ancient Greek 😊) was sent on a floppy disk to research institutions around the globe in 1989 and since then malicious computer programs have caused billions in damage to consumers, businesses, and governments.

It's been a challenging—and, at times, frightening—2021 year for cyber security pros with an array of high-profile breaches that have disrupted business operations, broken down supply chains and even led to business shutdowns. We've seen sophisticated attacks on governments by state sponsored entities. We've seen a decided increase in ransomware shutting down core infrastructure. We've seen supply chain breaches that impact hundreds, if not thousands, of downstream organizations. So, what do the recent attacks tell us about the state of security today and how can we learn from them?

HERE ARE MY TOP 5 CASES AND LESSONS FROM THE PAST 2021 YEAR'S MAJOR BREACHES.

1- SOLARWINDS
YOU NEED TO KNOW WHAT IT ASSETS YOU OWN AND WHERE THEY ARE, BECAUSE ATTACKS CAN COME FROM ANYWHERE, INCLUDING THE SUPPLY CHAIN.

THE FACTS:

In December 2020, cybersecurity firm FireEye announced they'd been the victim of a successful attack where their own Red Team toolkit was stolen; later that month FireEye informed SolarWinds that attackers had gotten into their systems via a backdoor planted in SolarWinds' Orion software update. APT29, a nation state actor associated with Russia intelligence agencies, essentially weaponized SolarWinds' commercial software by embedding malware in the Orion update and allowed the attackers to use the code almost as a form of trojan, getting into every device and system it's configured to monitor and manage.

LESSON LEARNED FROM SOLARWINDS

Attacks can come from anywhere, even the most trusted vendors in your supply chain, like SolarWinds. This is especially true when those vendors are targeted by highly sophisticated, state sponsored actors. That's why it's vitally important to know what IT assets you use and where they are. Having the knowledge of your assets, who owns them, and how critical they are to the business lets you respond quickly to risks to those assets. For the SolarWinds breach, if those impacted knew their attack surface, including the supply chain, then the moment that they were made aware of the breach they could see if they were impacted. This is in stark contrast to the hours, days, weeks that it might otherwise take.

Do you know where all your data is?
SharePoint, GoogleDrive, DropBox, Central storage, elsewhere.

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION Israel Institute of Technology
Tel: +972 48294192
glickstein.m@technion.ac.il \ cis.technion.ac.il

2- COLONIAL PIPELINE
IT'S TIME TO FOCUS ON FINDING REMOTE ACCESS SERVICES TO PROTECT AGAINST RANSOMWARE.

THE FACTS:

In early May of 2021 ransomware group DarkSide shut down 5,550 miles of petroleum pipeline, stranding barrels of gasoline, diesel and jet fuel on the Gulf Coast of the U.S. It appears that hackers gained entry via the company's VPN using a compromised password. The group has been operating their ransomware—called "DarkSide ransomware" and delivered as-a-service – against U.S. and European companies for at least half a year. Attackers using DarkSide's ransomware variant generally gain initial access by exploiting remote services like Citrix, Remote Desktop Web (RDWeb), or remote desktop protocol (RDP) from an external attack surface. Once they gain a foothold, they dig in deeper via lateral movement, exfiltrating data, and then encrypt everything with ransomware to extort money from their victims.

LESSON LEARNED FROM COLONIAL PIPELINE

Successful ransomware attacks are big business – even given that some of the Colonial ransom money was returned. The ROI for attackers of ransomware attacks like this one was estimated at 1,400%. Typically, these attackers perform reconnaissance, then, as noted earlier, they access the target via some type of remote access service. Then they go lateral to find and encrypt valuable assets. The pandemic has made it easier than ever for groups like DarkSide to find targets.

Ransomware attackers have become quite sophisticated this past year, "segmenting the market" and running large-scale campaigns against small and mid-size organizations, and more targeted campaigns against large organizations or those with mission-critical operations (i.e., hospitals, oil pipelines and local governments).

Given the confluence of big business and big dollars for attackers in ransom payments, the best defense is to ensure that you find and secure remote services. While this is easy to say, we know from experience that it's difficult to actually do without an external attack surface management solution to provide visibility, offer insights and help set priorities.

<u>It is important to connect remotely only using the Technion SSLVPN. At the end of the work disconnect from the network and if it is a non-private computer close all windows and if possible, also perform a shutdown or restart.</u>

3- MICROSOFT EXCHANGE VULNERABILITIES (OLD AND NEW!)
DON'T FORGET YOUR OLD GEAR... BECAUSE ATTACKERS WON'T.

THE FACTS:

A number of vulnerabilities in Microsoft Exchange Servers have turned up in 2021. Vulnerabilities targeting 2010, 2013, 2016 or 2019 servers. The vulnerabilities were reportedly used in multiple Zero Day exploits, in which they were used to gain access to email accounts and to plant additional malware.

All of the vulnerabilities mentioned above allow an authenticated attacker to write a file to any path on the server. While these flaws have likely been around for a long time, exploitation of them took off in January along with the press coverage. Over a matter of days the number of potential victims went from 30,000 to 60,000 or more.

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION Israel Institute of Technology
Tel: +972 48294192
glickstein.m@technion.ac.il \ cis.technion.ac.il

LESSON LEARNED FROM MICROSOFT EXCHANGE

As you can see, some of these are for older systems, and in the case of the Exchange 2010 servers, hardware/software that is no longer supported by Microsoft. **The number one lesson here is don't forget your old gear… because attackers won't.** You should be continuously monitoring your entire external attack surface for security gaps, even on the older gear.

In addition, even if a company has upgraded or replaced systems that are at risk, you must not assume that everyone that you do business with has followed suit. A small subsidiary of one of your third-party suppliers may not ever think of replacing a server that's working "perfectly well." Ditto for your partners.

Do not allow any outsider to connect to your computers without the supervision of the IT team

4 ACCELLION

BRUSH UP YOUR BREACH DISCLOSURE POLICY AND BE SURE THAT WHEN CONFRONTED WITH A PROBLEM (LIKE A BREACH), YOU TELL THE WHOLE TRUTH.

THE FACTS:

Accellion engaged 3rd Party in March 2021 to investigate earlier attacks on their legacy File Transfer Appliance (FTA). Accellion, which **had quietly issued a patch** in December, failed to point out the severity of possible exploits. The attack used a combination of zero-day attacks to extract data which was then held for ransom. The attackers began to issue extortion letters in January. Victims were customers and even the customers of Accellion customers, including major financial and healthcare institutions, as well as a number of universities and global retailers.

LESSON LEARNED FROM ACCELLION

One of the biggest lessons learned from the Accellion breach is one that your Mom may have taught you: "Tell the whole truth". The most consistently reported topic related to the breaches is that Accellion tried to downplay the issues and consequently gave themselves a black eye. Breaches continued to emerge months after the actual exploit because organizations didn't have the right info on how to prioritize the risk.

This series of events also serves as a reminder that it's best to have forthright breach disclosure rules in place before a breach happens. And, again, it's important to fully explain what went wrong.

If you suspect an incident, do not hesitate and report immediately to the security trustee of your unit or directly to CISO.

5 FLORIDA AND CALIFORNIA WATER UTILITIES HACKS

THE STAKES CONTINUE TO GO UP SO IT'S IMPORTANT TO STAY VIGILANT.

THE FACTS:

In February 2021 a water treatment plant employee in Oldsmar, Florida noticed that someone else was remotely controlling his computer. Apparently, this behavior in itself was not alarming given remote access is commonly employed to troubleshoot IT, but what was alarming was the person on the controls tried to turn up the amount of lye (sodium hydroxide) in the water to dangerous levels. Fortunately, the employee was able to act quickly and mitigate what could have been a dangerous and life-threatening breach.

Meanwhile, unbeknownst to the world, in January 2021 another water system, this time in San Francisco, California, was similarly compromised. Again, the water utility was accessed by the attackers using an employee account in TeamViewer, third party software which allows

connectivity between computers for remote access and support. The attacker, once logged in, proceeded to delete programs for treatment of drinking water. The attack was discovered quickly—the next day.

LESSON LEARNED

This last batch of threats are designed by attackers to inspire fear, as they target a piece of life sustaining and critical infrastructure—water utility systems. Combine these with the Colonial Pipeline shutdown of a key U.S. oil pipeline and ransomware attacks on hospitals and we see that there does not appear to be a moral or human limit to what attackers will do, and what systems they are willing to shut down if they are not paid. In this atmosphere, it's important that security leaders and end users continue to stay vigilant and do everything they can to prevent attackers from getting into their systems in the first place.

The question from previous newsletter

Your computer has just been infected with Ransomware and the hacker is demanding money before releasing it. What do you do?

A - Send an email to the IT guy in the office.

B - Try your best to get rid of it before anyone finds out

C - Pay the ransom. You need your files back!

D - Disconnect your computer from the network

The correct answer is "D" – This is the first thing to be done. It disconnects the attacker from your computer. Once done the technical treatment can start. Bonus explanation - Shutting the computer done may trigger unwanted processes after restart or erase artifacts.

New question:

Who is responsible for information security in the Organization?

A. Chief Executive Officer - CEO

B. Chief Information Officer - CIO

C. All users

D. Chief Information Security Officer and Information Security Trustees - CISO

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION Israel Institute of Technology

Tel: +972 48294192

glickstein.m@technion.ac.il \ cis.technion.ac.il