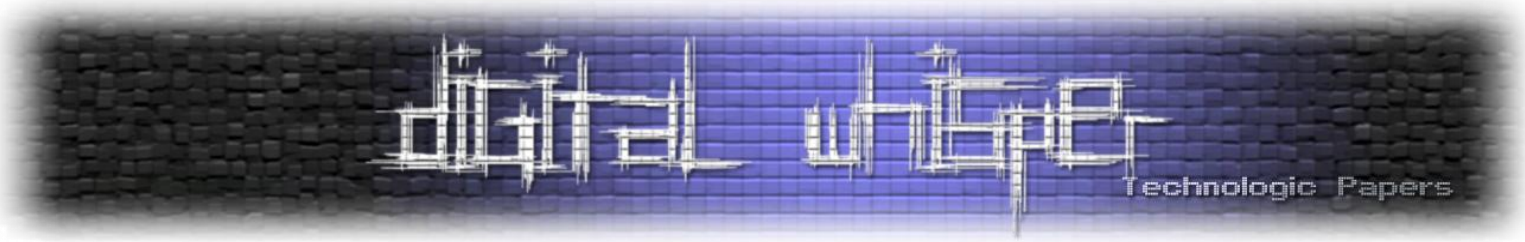


DNS Rebinding

מאת אביעד (greenblast)

הקדמה

מאמר זה עוסק בהתקפת DNS Rebinding. להבנת המאמר נחוץ ידע בסיסי בדרכי פעילות האינטרנט ובפרט פעילות ה-DNS, אני ממליץ לקרוא את ההקדמות למאמר של אפיק קסטיאל בנוגע ל-"DNS Cache Poisoning" מהגיליון השני של Digital Whisper, שם מפורט בקצרה על דרך הפעולה של DNS. במאמר אתייחס בעיקר לדוגמאות משפת JavaScript, אך המתקפה נוגעת גם לשפות צד לקוח אחרות כגון Flash ו-Java applets.

(SOP) Same Origin Policy

בכל פעם שאנחנו מתחברים לאתר אינטרנט, הדפדפן שלנו מוריד קטעי קוד מסויימים שרצים על המחשב שלנו בידי הדפדפן (HTML, Javascript וכד'). הדפדפן הוא זה שקובע כיצד האתר יוצג למשתמש. כאשר האתר שהתחברנו אליו נמצא תחת שליטה של מישהו בעל כוונות זדוניות, הוא יכול לגרום לדפדפן להריץ קוד ולבצע דברים כדי לקדם את מטרותיו. כמובן שהדפדפנים מתוכננים כך שימנעו ביצוע של קוד זדוני, חלק מיכולת ההגנה של הדפדפנים באה לידי ביטוי במנגנון ה-Same Origin Policy.

SOP הנה מדיניות אבטחה המיושמת ברב בדפדפנים המודרניים, ונוגעת למספר שפות תכנות מבוססות דפדפן (הדוגמא הכי נפוצה, Javascript כמובן). מדיניות זו מביאה ליצירת "ארגזי חול" נפרדים לאתרים שונים ומונעת מהם לתקשר ביניהם. כמו כן, קובעת המדיניות כי כל דף יהיה מסוגל לתקשר אך ורק עם השרת ממנו הוא הגיע. ללא מדיניות זו, כל אתר שנבקר בו יוכל להשתמש ב-JavaScript כדי לתקשר עם כל אתר אחר, והדבר בעייתי מסיבות שונות, לדוגמא:

- אתר זדוני יוכל להשתמש בדפדפן כצעד ביניים בדרך להתקפות נוספות (כפרוקסי למשל.)
- אתר זדוני יוכל לנצל את משאבי המערכת שלך (CPU וקישוריות לאינטרנט)

- במידה ואנו מחוברים לאתר אחר הדורש הרשמה והתחברות, כאשר קוד זדוני רץ על הדפדפן, התוקף יוכל לתקשר עם האתר תוך כדי שימוש במזהים שלנו (לא נעים כשמדובר במשהו קריטי כמו בנק)

כמובן שאף אחד מהתרחישים שהוזכרו כאן אינם מקובלים ולכן הדפדפנים עושים את מירב המאמצים למנוע פעולות כאלה.

הטבלה הבאה שנלקחה מויקיפדיה מתארת את הגישה שיש לפונקציית JavaScript הנמצאת ב:
www.example.com

Compared URL	Outcome	Reason
http://www.example.com/dir/page.html	Success	Same protocol and host
http://www.example.com/dir2/other.html	Success	Same protocol and host
http://www.example.com:81/dir2/other.html	Failure	Same protocol and host but different port
https://www.example.com/dir2/other.html	Failure	Different protocol
http://en.example.com/dir2/other.html	Failure	Different host
http://example.com/dir2/other.html	Failure	Different host (exact match required)
http://v2.www.example.com/dir2/other.html	Failure	Different host (exact match required)

בנוסף לבעיות שהוזכרו, תוקפים יכולים לנסות בעזרת קוד זדוני לנצל את היכולות שמוענקות לנו על ידי מיקום פיזי. לדוגמא, כאשר אנחנו גולשים באתרי אינטרנט מהעבודה, התוקפים אמנם אינם יכולים לראות ישירות את שרתי האתרים הפנימיים של החברה אך הם יודעים שאנו יכולים לראות אותם. מכיוון שנקודת המבט של מחשב היושב מאחורי ה-firewall של הארגון שונה מאוד מנקודת מבט של מחשב באינטרנט, אם איכשהו תתאפשר לתוקף הסתכלות למה שאנו רואים, יכולתם ההתקפית תשתפר. בהמשך נדון כיצד ניתן לבצע התקפה שתאפשר הסתכלות כזאת.

המדיניות ברוב המקרים לא חוסמת שליחת מידע מהאתר לאתר אחר, אלא בעיקר חוסמת את התגובות מאתרים. כעת ניתן להבחין בגורם לבעיה רצינית עם המדיניות, היות והיא עצמה מתייחסת רק לשמות-hostname והאינטרנט כפי שידוע לנו, מבוסס על כתובות IP!

מעורבותו של ה-DNS

כדי להתחבר לאתר מסויים, ברוב המקרים הדפדפן מקבל תחילה כתובת הגיונית (hostname, לדוגמא: www.yoursite.com) את הכתובת הזו הדפדפן צריך להמיר לכתובת IP מובנת, כדי שיהיה ניתן ליצור התקשרות איתה, המרה זו מתבצעת באמצעות שירות ה-DNS. אז במילים פשוטות, לשם רענון, התהליך הוא כזה:

1. משתמש מכניס כתובת www.yoursite.com
2. הדפדפן שולח שאלה ל-DNS: מה ה-IP של האתר הנ"ל?
3. DNS מחזיר תשובה 111.111.111.111
4. דפדפן מתחבר ל-111.111.111.111

הבקשה שהדפדפן ישלח אם כן ל-111.111.111.111 IP תיראה בערך ככה:

```
GET / HTTP/1.1
Host: www.yoursite.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
rv:1.8.1.1) Gecko/20061204 Firefox/2.0.0.1
Accept: */*
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
```

כל תשובה מ-DNS מגיעה עם שדה TTL (Time To Live) שמגדיר בדיוק כמה זמן המידע שנשלח חזרה תקף מבחינה רשמית . שרת ה-DNS מצפה מהדפדפן לא לבצע בקשות נוספות בנוגע לאותו אתר ספציפית. הדפדפן שומר בזיכרון את הקשר hostname-IP עד הכיבוי שלו, או כל עוד הוא חושב שהקשר עדיין תקף. במקרה של רוב הדפדפנים, הקשר תקף לכמות הזמן שרשומה ב-TTL, ובדפדפנים מסוימים (IE) מתווספת על ה-TTL כמות זמן מסוימת (במקרה של IE מדובר ב-30 דקות). תוספת זמן זאת נקראת DNS Pinning.

DNS Pinning קיים גם למטרות אבטחה, זאת על מנת למנוע מצב של מניעת שירות או שינוי ה-IP דרך ה-DNS, כמו גם לספק למשתמש עבודה רצופה מול האתר. עם זאת, תוספת האבטחה שהוא מעניק מוטלת בספק (תיכף נסביר למה) והיא תוספת של נוחות ומניעת הצורך בשאילתות נוספות בלתי נחוצות ל-DNS.

במידה ויתבצעו שינוים בהגדרות ה-DNS, תוך כדי שהמשתמש עדיין מחובר לאתר האינטרנט, הדפדפן ימשיך להשתמש בערכים המקוריים. אולם במקרים בהם הדפדפן מסיבה כלשהי אינו מצליח להגיע לאתר שמקושר אצלו בזכרון לפי יחס ה-hostname-IP, הדפדפן יניח שחל שינוי כלשהו ויבצע את תהליך שאילת ה-DNS וקישור ה-hostname-IP מחדש בהתאם לתשובה שיקבל. זאת תוכנית הפעולה המקורית, בעולם ללא תוקפים זדוניים.

התקפה: מה מנסים לעשות, ולמה ה-DNS Pinning מפריע

כעת נשוב לעולם בו קיים מישהו זדוני.

מטרתו של התוקף היא בהתחלה להפנות את ה-hostname המקורי לכתובת ה-IP שלו ולאחר מכן, כאשר הקוד הזדוני שנמצא באתר שלו רץ על הדפדפן ולהחליף את כתובת ה-IP שלו לכתובת שהוא רוצה להריץ עליה את שאר הקוד , דבר זה יאפשר ל אותו תוקף לעקוף את ה -SOP. עלינו לזכור שה-SOP מתייחס ל-hostnames ולא ל-IP כדי לקבוע מה מותר ומה לא , כך שכל שינוי של האתר , מבחינת ה-IP (וכל שאר הבחינות חוץ מה-hostname) יאפשר הרצה של קוד בלי הגבלה במקומות שלא אמורים להיות לו גישה אליהם, כמו שרתי אתרים פנימיים של החברה.

כיצד DNS Pinning מפריע להתקפה

הנה תרחיש של מתקפה אשר תכשל:

- התוקף מתפעל אתר www.evil.com על כתובת ה-IP: 111.111.111.111 ושרת DNS, בשביל שאילתה על www.evil.com השרת יחזיר 111.111.111.111 עם TTL קצר, לדוגמא שנייה אחת (אפשרי לנסות אפילו פחות, אבל לא תמיד כדאי כי התוקף תלוי במהירות הדפדפן וחיבור האינטרנט של הקורבן)

- משתמש מחליט לבקר ב-www.evil.com ובהתאם לתשובתו של שרת ה-DNS הדפדפן יופנה ל: 111.111.111.111, מוריד ומבצע את תוכן הדף (במקרה שלנו, דף הבית של האתר). על דף זה קיים קוד JavaScript שמחכה 2 שניות (כפול מהזמן שנקבע ב-TTL) ומורה לדפדפן להתחבר מחדש (XHR) ל-www.evil.com (אין שום בעיה עם הדבר, מאחר ומדובר ביחס hostname-SOP זהה) אולם בזמן החיבור , ההגדרות בשרת ה-DNS ישתנו וכתובת ה-IP שמוחזרת כתשובה על www.evil.com תשתנה לכתובת 10.10.10.10, שאנו נניח שהיא הכתובת www.target.com, אותה התוקף רוצה לתקוף.

- ההתקפה נכשלת, מכיוון שתהליך ה-DNS Pinning שימר את הכתובת www.evil.com לכתובת ה-IP: 111.111.111.111. דבר זה כמובן מנוגד לרצונו של התוקף , היות ובמקום להתחבר ל-10.10.10.10 הדפדפן של הקורבן יתחבר שוב פעם לכתובת ה-IP: 111.111.111.111 מבלי לבצע שאילתת DNS נוספת.

במידה וההתקפה היתה מצליחה, הדפדפן היה שולח ל-10.10.10.10 בקשה מעין זו:

```
GET / HTTP/1.1
Host: www.evil.com
User-Agent: Mozilla/5.0 (Windows; ; Windows NT 5.1; rv:1.8.1.14)
Gecko/20080404
Accept: */*
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
```

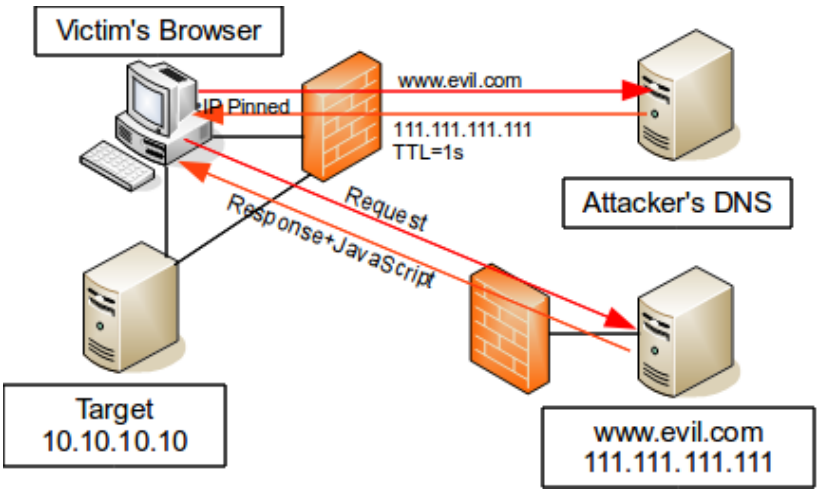
כביכול, נראה כי גם אם התוקף יעקוף את בעיית ה-Pinning, קיימת עדיין הבעיה ששדה ה-Host מתייחס ל-www.evil.com ולא ל-www.target.com. מסתבר שאין חשיבות גדולה לדבר, מכיוון ששרתים גדולים רבים מוגדרים להקשיב לכל Host header, כך שהתוקף בסופו של דבר כן יוכל לשלוח בקשות בצורה זו. יש לשים לב שבכדי לתקוף את הכתובת, התוקף צריך לדעת שהיא קיימת. במקרה ובו מדובר בכתובת פנימית בתוך רשת של חברה מאחורי FireWall, התוקף צריך לבצע התקפות enumeration מקדימות כדי לדעת לאן לתקוף. אולם במקרים רבים קיימות כתובות פנימיות מוכרות, כך שניתן לתקוף אותן גם בלי ידע מוקדם (192.168.*.* או 10.*.*.*)

DNS Rebinding נגד ה-Pinning

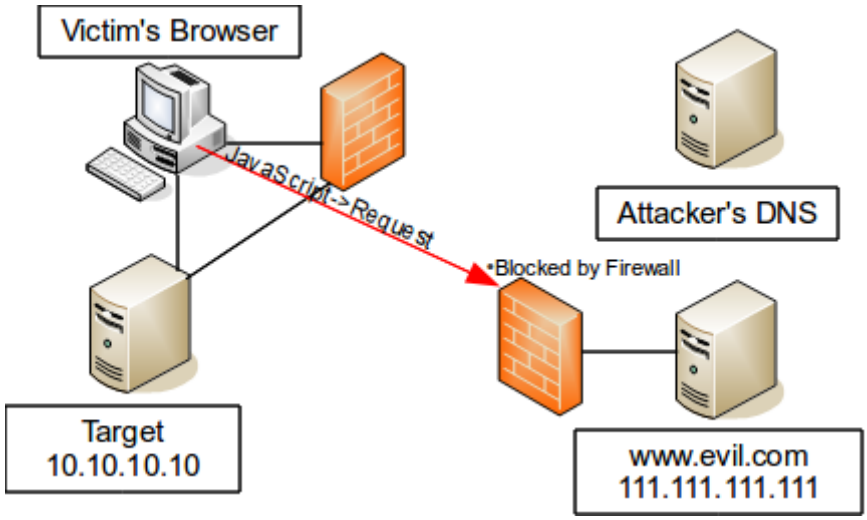
במקרה ודפדפן עם Pinning לא מצליח להגיע לאתר כלשהו, היכולת לתשאל את ה-DNS ולבצע קישור מחדש של ה-IP, היא שימושית ביותר, מכיוון שמדי פעם כתובת IP של אתרים אכן משתנה. לעומת זאת, יכולת זו עשוייה להביא לפרצת אבטחה חמורה. ניתן להניח שכאשר אתר רגיל בלתי ניתן להגעה, הדבר נובע מסיבה הגיונית ולא בכוונה, אולם הדבר לא כך כאשר מדובר באתר זדוני, שיכול להיות מנוטרל לפי רצונו של התוקף.

הנה תרחיש הממחיש כיצד ניתן להשתמש ב-DNS Pinning להגעה אל אתרים מאחורי FireWall:

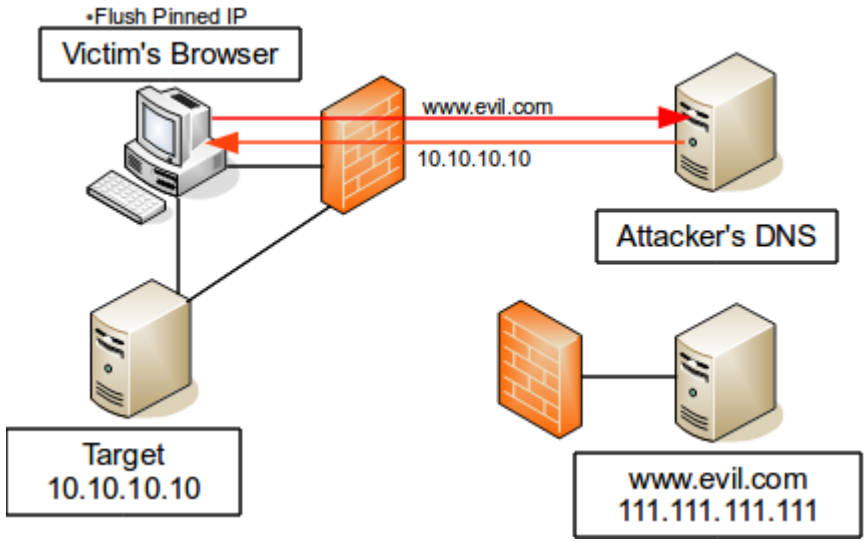
- כמו בפעם הקודמת, המשתמש מתחבר ל-www.evil.com תוך שימוש ב-IP 111.111.111.111 עם TTL של שניה.



- הדפדפן מוריד דף שמכיל קוד JavaScript המורה לו להתחבר מחדש לאתר כעבור 2 שניות
- מיד לאחר שהדף הגיע לקורבן, האתר התוקף מונע גישה מהקורבן לאתר, בעזרת שימוש ב-FireWall לדוגמא.



- הדפדפן שלא מצליח להתחבר מחדש לאתר, מחליט לאפס את מנגנון ה-Pinning.
- הדפדפן שואל את ה-DNS איזה כתובת IP יש ל-www.evil.com עכשיו.

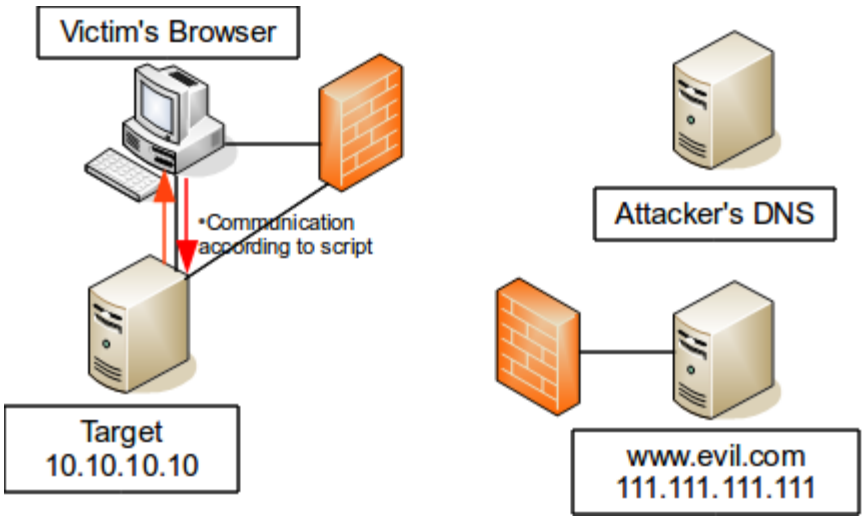


- ה-DNS עונה עם ה-IP 10.10.10.10, הכתובת של האתר www.target.com שיכול להיות גם באותה רשת פנימית שבה נמצא הדפדפן של הקורבן, רשת פנימית שיכולה להיות גם מאחורי FireWall שמונע גישה.

- האתר שולח ל-10.10.10.10 את הבקשה שראינו לפני כן:

```
GET / HTTP/1.1
Host: www.evil.com
User-Agent: Mozilla/5.0 (Windows; ; Windows NT 5.1; rv:1.8.1.14)
Gecko/20080404
Accept: */*
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflateאט
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
```

- השרת ב-10.10.10.10 מגיב בהתאם (דף הבית של www.target.com לדוגמא)



- הדפדפן מקבל את המידע, ופועל בהתאם לפקודות שקיימות בסקריפט שעדיין רץ, כמו למשל שליחה של המידע על ידי טופס POST לשרת אחר של התוקף.

שמה של המתקפה נובע מתהליך הקשירה מחדש של ה-IP ל-hostname. (בהתחלה שם המתקפה היה Anti-DNS Pinning, אבל השם שנקלט היה DNS Rebinding)

מה הרווח?

כפי שניתן לראות, ביצוע המתקפה מאפשר לתוקף להריץ שורות סקריפט על העמדה המקומית תוך כדי עקיפת מנגנון ה-Same Origin Policy ובעצם לגרום לדפדפן של הקורבן לבצע פעולות בשביל התוקף.

הנה כמה דוגמאות למה שניתן לבצע בעזרת המתקפה:

עקיפת FireWall

- ראינו שניתן להגיע בעזרת המתקפה מהאינטרנט לשרתים פנימיים בתוך ה-Intranet של האירגון שיכולים להיות גם מאחורי FireWall. בעזרת המתקפה ניתן לבצע זחילה על ה-Intranet ולבצע בסקריפט ניסיון לה גיע לשרת Web בתוך ה-Intranet, ממנו אפשר לבצע מעקב אחרי קישורים שונים בכדי למפות את הרשת הפנימית.

- ניתן לבצע בדיקות לפרצות ידועות במשאבים השונים ב-Intranet. וכמובן, לנסות לבצע פעולות נוספות באמצעות הפרצות. למעשה, ניתן לנסות לפרוץ בעזרת כך למחשב הקורבן עצמו ומכיוון שמקור ההתקפה יתבצעו מה-localhost יכול להיות שבידי התוקף לבצע מעקפים להגנות שונות. בעזרת מהלך זה, ניתן לשמור על נוכחות בתוך הרשת הפנימית אפילו לאחר שהמשתמש סגר את הדפדפן.

- התוקף גם יוכל להשתמש לרעה בשירותים הנגישים מתוך הרשת הפנימית, כגון שירותי הדפסה שלפעמים אינם דורשים הרשאות בגישה מהרשת הפנימית וגישה ל-FTP פנימיים שהוגדרו כי ניתן לגשת אליהם ללא זיהוי (מתוך המחשבה ש-"מכיוון שהם פנימיים לא ניתן להגיע אליהם מרשת האינטרנט"). בנוסף יש סיכוי שנתבים בתוך הרשת הפנימית הושארו עם סיסמאות ברירת המחדל שלהם. חשוב לציין כי הרבה נתבים מכילים הגנה ב-Firmware נגד XSS ו-XSRF, במיוחד על מנת למנוע שינוי של ההגדרות אצלהם, אולם בעזרת המתקפה הנ"ל יהיה ניתן לגשת אליהם בגישת socket direct. בגליון זה אפשר לקרוא את המאמר של אביב ברזילי על החולשות בפרוטוקול UPnP בכדי לקבל הסבר מצוין על הנושא.

IP hijacking

- ניתן להשתמש במתקפה בכדי לתקוף מטרות ברחבי האינטרנט עצמו, לבצע Click frauds ולנסות לרמות את האלגוריתמים שנכתבו ע"מ למצוא הקלקות בלתי תקינות. הדבר דורש אמנם תעבורה גדולה לאתר שמשתמשים בו להתקפה, אך כמעט ברוב המקרים הרווחים במתקפה כזאת עולים על ההשקעה שבהקמה ותחזוקה של אתרים ספציפיים שיכולים לייצר תעבורה מרובה (ויש אנשים שמבינים בדיוק על איזה אתרים אני מדבר).

- לשלוח Spam מ-IP שיש לו מוניטין נקי ולא נחסם על ידי רשימות שחורות. אמנם ברוב הדפדפנים פורט ה-SMTP חסום, אך ניתן לבצע שליחות בעזרת DNS Revbinding דרך טכנולוגיות כגון JAVA או Flash, שאצלהם השירות מותר. מדי פעם התוקף יוכל להשתמש בממסר המייל של הקורבן עצמו, במידה והקורבן משאיר אותו מחובר ופתוח (למטרות polling לדוגמא).

- ביצוע Fixation Session על מנגנוני זיהוי מסוגים שונים. למרות שהדבר אינו מומלץ על ידי מומחי אבטחה, עדיין קיימים מפתחים אתרים שמבצעים אימות על ידי IP. במידה ומדובר במנגנוני אימות

שונים, ניתן אף למצוא דרכים לפתור את הבעיה (B-day attack לדוגמא, במקרה בו קל לנחש את ערכי ה-cookie).

- שימוש במחשב הקורבן כשרת פרוקסי, כך ניתן לבצע בעזרת הדפדפן של הקורבן התקפות שונות למטרות שונות. לדוגמא, עקיפת מנגנוני ה-captcha של גוגל שמופיע במקרים מסויימים כאשר IP מסויים מנסה לבצע פעולה מחזורית, על ידי שימוש בקורבנות רבים, לכל אחד מהם IP שונה. ניתן אפילו להפליל אדם מסויים ולגרום למחשב שלו לבצע עברות שונות.

דרכי התגוננות

דרך התגוננות ראשונה , כפי שניתן ללמוד מהמתקפה עצמה , היא להגדיר את השרתים והמכשירים ברשת, לייחס חשיבות עליונה לשדה ה-Host ולאשר בקשות שמגיעות רק מ-Host שנמצאים בתוך הרשת הפנימית.

לצערנו, כמעט תמיד אין מדובר באפשרות ריאלית. פירוש הדבר שצריך להגדיר זאת לכל משאב רשת כגון: מדפסת, ראוטר, שרת, טלפון מבוסס IP או כל מכשיר אחר אשר מסוגל להתחבר לרשת הפנימית ועושה זאת. לא כל המכשירים תומכים באפשרות הזאת ולפעמים אף יכול להיות שהדבר יפריע לפעילויות שונות ברשת הזקוקות למדיניות פתוחה יותר בנוגע ל-hostnames. למרות הבעייתיות שבדבר, על ארגון להעדיף מכשירים שכן מסוגלים לתמוך באפשרות כזאת על פני מכשירים שלא, ולנסות לצמצם את כמות המכשירים הפגיעים ככל שניתן. כמו כן יש אפשרות לעשות שימוש במזהים נוספים, כמו cookies, מזהים שכאלה יכולים להוסיף ליכולת להתגבר על הפרצה אך אין לסמוך עליהם בלבד, מכיוון שבהרבה מקרים כן ניתן לעקוף את ההגנה שהם מספקים בעזרת אמצעים שונים (כגון מתקפות 0-day, שימוש ב-plug-ins בהם דרך השימוש שונה).

בנוסף על השיטה שהוזכרה במאמר זה, צריך לזכור תמיד שגם אם שירות או מכשיר כלשהו נמצא ברשת הפנימית, אפילו מאחורי firewall, עדיין יש דרכים ופרצות אבטחה שמאפשרות להגיע אליו. על כן, נגדיר סמאות אבטחה בסיסיות לכל השירותים שאליהם הדבר אפשרי , גם במקרים בהם הם נראים מנותקים וירטואלית מהאינטרנט. לדוגמא, לא נאפשר שירותי FTP אנונימיים, ונשנה את סיסמאות ברירת המחדל גם בנתבים שנמצאים מאחורי firewall ברשת הפנימית.

נתקלתי ברשת בראיון עם חוקר/מומחה/יועץ האבטחה דן קמינסקי, הידוע בין השאר בזכות שלל הגילוים והמחקרים שלו בתחום מתקפות ה-DNS Cache Poisoning ו-DNS Rebinding. הראיון עסק בעיקר ב- DNS Rebinding וההשלכות שלו על ארגונים. בראיון הציע דן להתחיל לייצר מכשירי רשת שדורשים אימות נוכחות פיזי של משתמש לידם , לפני ביצוע שינויי הגדרות קריטיים שעלולים להיות זדוניים . למשל, נתב שלפני שינוי הגדרות דורש מהמשתמש לנתק כבלים מסוימים כדי להוכיח שהמשתמש הנוכח פיזית מנסה לשנות את ההגדרות , ולא שירות חיצוני מרוחק שעלול להיות זדוני (כמובן שהוא הזכיר , שהדבר לדעתו מאובטח כי הוא עדיין לא נתקל בפקדי ActiveX שמסוגלים לנתק ולחבר כבלים בצורה טלקינטית , ברגע שהדבר יהיה קיים, כנראה שנצטרך לחשוב עוד קצת). שיטה נוספת, היא להשתמש ב-SSL גם לחיבורים פנימיים בתוך הרשת. במקרה ותתבצע התקפה, תקפוץ התראה בדפדפן שיש חוסר התאמה בין שדה ה-

Host של הבקשה לשדה התואם בתעודה. במקרה כזה, עדיין ישנו הצורך שהמשתמש עצמו יהיה מודע לאבטחה ולא ילחץ המשך הלאה בדף האזהרה, אחרת המתקפה תוכל להמשיך.

דרכי התגוננות אלה הן דרכים בסיסיות שאנו, כמשתמשים פשוטים או אחראי אבטחה בארגונים, יכולים להשתמש בהן בכדי להקטין את הסיכון. ניתן להמשיך לפרט על שיטות התגוננות נוספות מורחבות יותר הכוללות תיקוני מדיניות שונים לדפדפנים, שירותים, רשתות או רכיבי plug-in כדי למנוע פרצות מוגדרות. במאמר זה לא פירטנו על תיקונים אלה מכיוון שהם דורשים התעסקות ברמה עמוקה יותר עם הרכיבים הנוגעים לפרצה.

הבעיה הגדולה עם הפרצה, היא שניתן לבצע תיקונים מתאימים לדפדפן או ל-plug-in, אך שורש הבעיה נעוץ בדרך פעולתו של ה-DNS, כך שטיפול נקודתי יעיל רק לאזור מוגבל ביותר של הפרצה.

סיכום

DNS Rebinding היא מתקפת Man In The Endpoint (או Man In The Browser). המתקפה מבוססת על חוסר התיאום בין מנגנון ה-SOP למנגנוני ה-DNS בשרתי האינטרנט ובדפדפנים. בעזרת המתקפה התוקף יכול להשיג גישה למקומות אליהם לא קיימת גישה מרשת האינטרנט (ברשת פנימית) או לגרום לדפדפן של המשתמש לבצע פעולות בשביל התוקף, עם היתרונות המרובים שיש לתוקף בדבר. בגלל שמקור הבעיה הוא בדרך בה פועלים שירותי ה-DNS ומדיניות ה-SOP, יש בעיה רצינית כיום לטפל בפרצה בצורה גורפת ורב הפתרונות הקיימים כיום הם נקודתיים ולא מכסים את היקף הבעיה. למרות הזווית הפסימית, ישנה מודעות גדולה יותר למתקפה כיום ומתבצעים מחקרים רבים בנושא, בתקווה לשינויים משמעותיים באזורים הנוגעים לפרצה.

קישורים

http://vimeo.com/7907871 - הסבר מצויין של רוברט האנסן על המתקפה.

/dns/http://crypto.stanford.edu - מחקר של אוניברסיטת סטנפורד בנושא.