

# NTLM Relay Is Dead?

---

## No!

# About us

---

Yongtao Wang - @Sanr



- Co-Founder of Qihoo360 PegasusTeam.
- Specializes in penetration testing and wireless security.
- A lecturer at the China Internet Security Conference (ISC) security training camp.
- Blackhat, Codeblue, Poc, Kcon, etc. Conference speaker.

Back2Zero

Yang Zhang - @izy

- Back2Zero/XDSEC Team.
- Independent Security Researcher.
- Currently focusing on web application security, cloud security, windows security.

# TL;DR

---

- NTLM basic
- NTLM reflection attack history
- New technology to perform NTLM reflection attack
- A whole new perspective in SSRF
- Critical security issue in JAVA
- The new era in NTLM Reflection



# Let's Talk About NTLM



# NTLM Authentication

---

- NT LAN Manager: Suite of security protocols NTLM
- Network authentication for Remote Services
- Challenge-Response authentication mechanism



# NTLM Authentication

---

- Supported by the NTLM Security Support Provider on Windows
- NTLMv1/ NTLMv2/ NTLM2 Session
- HTTP, SMB, LDAP, MSSQL, etc.



# NTLM Type 1 Message

---

Client Request - NTLMSSP\_NEGOTIATE



# NTLM Type 2 Message

---

Server Response - NTLMSSP\_CHALLENGE



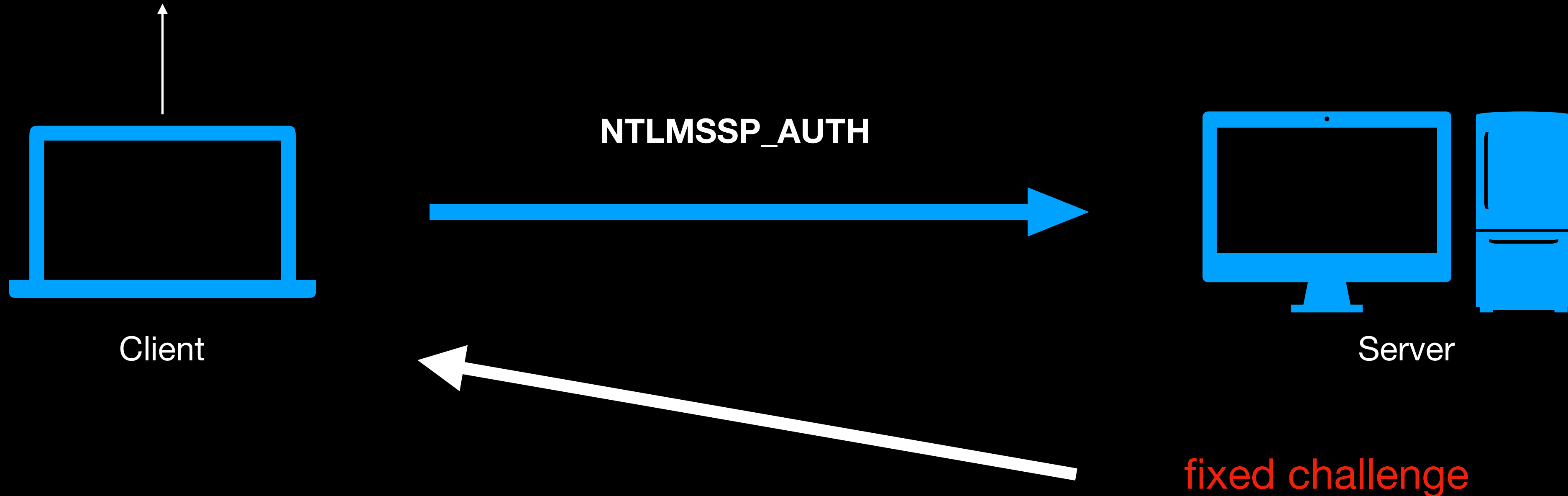


# NTLM Type 3 Message

---

Client Request - NTLMSSP\_AUTH

Net-NTLM = f(Challenge, NTLM Hash)

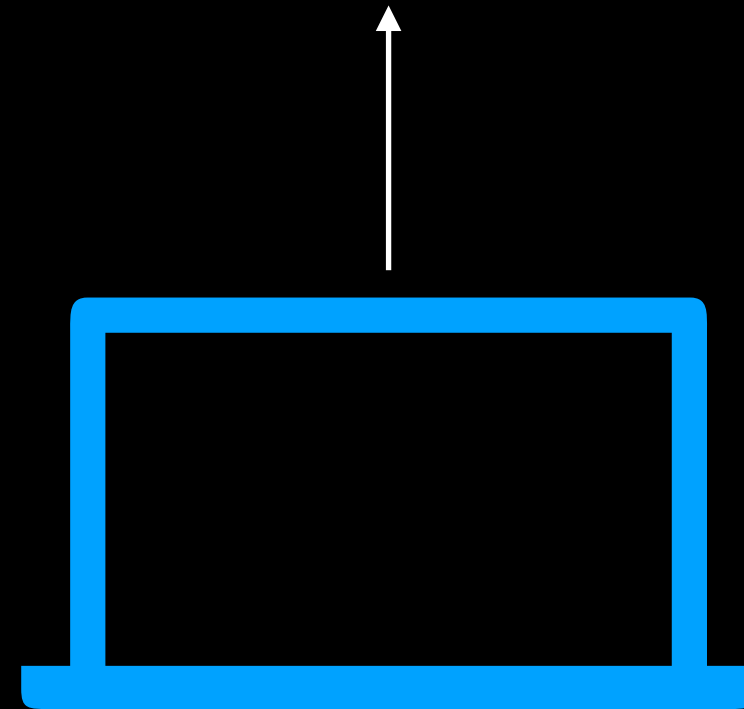


# NTLMv2 Type 3 Message

---

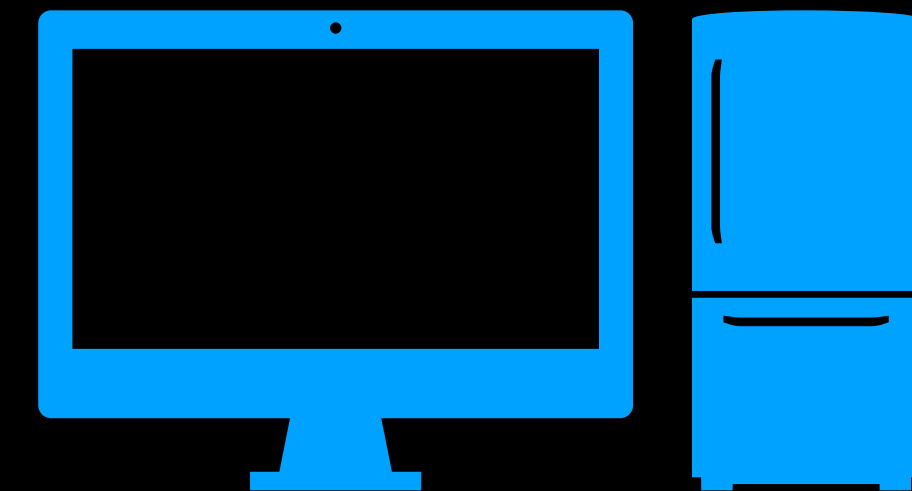
Difference in NTLMv2 and NTLMv1

Net-NTLM = f(Challenge, NTLM Hash, **Client Challenge**)



Client

Add client challenge to NTLMSSP\_AUTH



Server



# SMB -> SMB Reflection Attack



# NTLM Reflection

---

## SMB Reflection - SMB->SMB

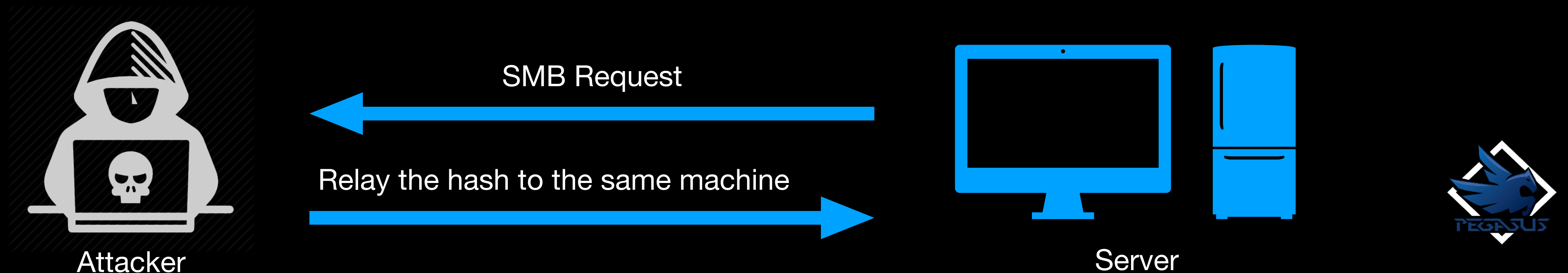
### Steps to reproduce:

Visiting an attacker's Web site with file:// in HTML.

The browser will authenticate to attacker automatically.

(There are many ways to get an SMB request)

### Relaying the Net-NTLM HASH to the same machine (SMB Reflection)



# NTLM Reflection

---

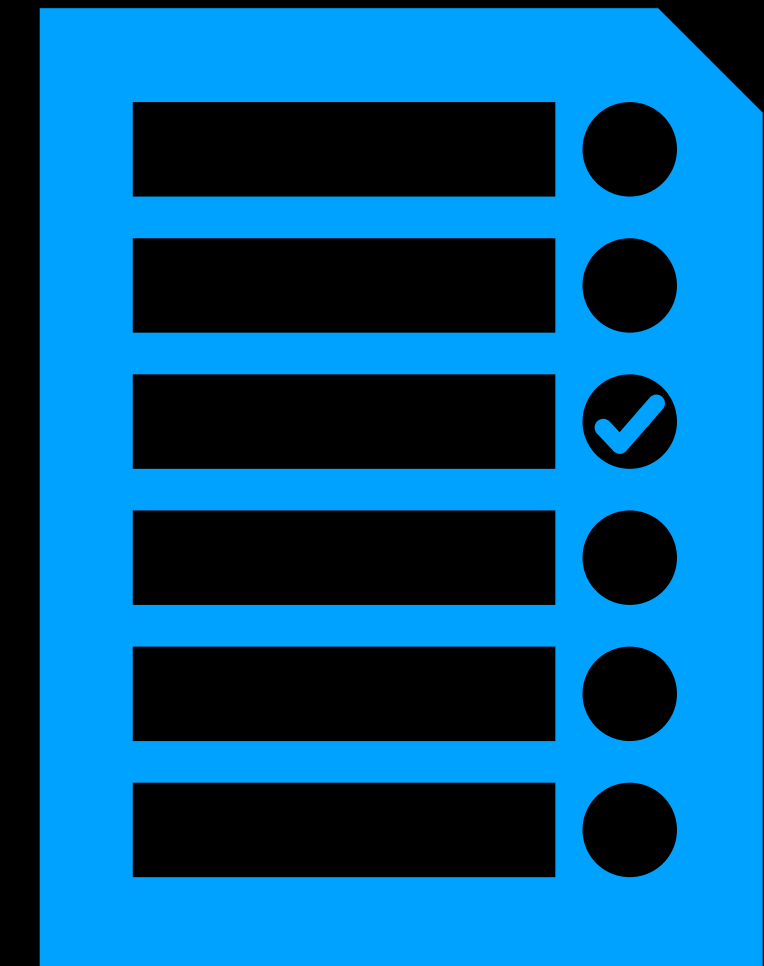
SMB Reflection - MS08-068

**Microsoft issued a *partial* fix (MS08-068)**

Stop relaying back to itself finally.

***Can not stop Attacker from***

Relaying the Net-NTLM Hash to another machine or  
Perform Cross-Protocol Reflection attack.



	✓

Active Challenge Table



# HTTP -> SMB Reflection Attack

Cross-Protocol Reflection



# NTLM Reflection

---

Hot Potato - HTTP->SMB Reflection

***Combined 3 vulnerabilities to perform Privilege Escalation***

1. NetBIOS Name Service Spoofing
2. Web Proxy Auto-Discovery (WAPD) MITM Attack
3. HTTP->SMB Reflection Attack



# NTLM Reflection

---

Hot Potato - HTTP->SMB Reflection

## ***6 Steps To Reproduce (Windows 7)***

1. Start NBNS Spoofing to hijack WAPD
2. Start a Web Server on localhost:80
3. Redirect Windows Defender Update request to `http://localhost/GETHASHxxx`
4. Send 401 Response to Windows Defender Update
5. Windows Defender Update will authenticate to us with SYSTEM account automatically.
6. Send the Net-NTLM Hash to Samba Service

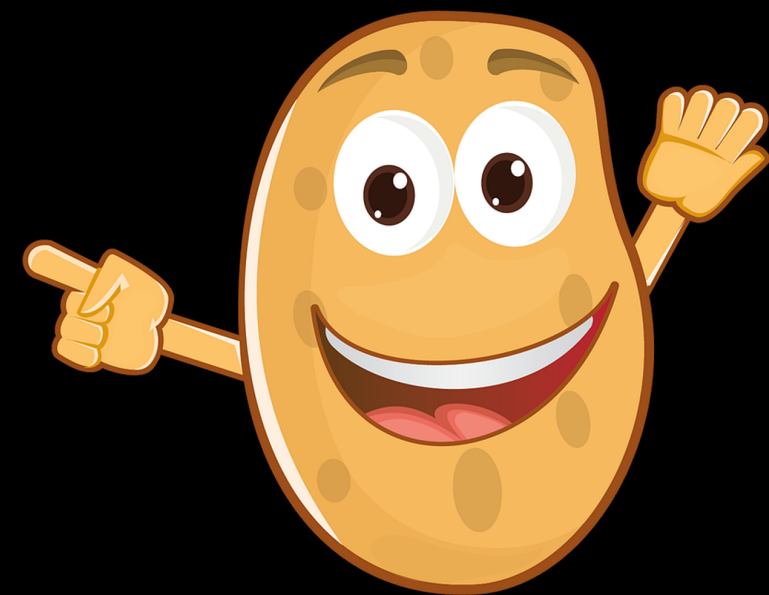




# NTLM Reflection

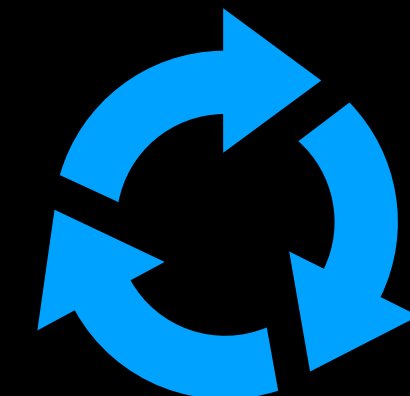
---

Hot Potato - HTTP->SMB Reflection



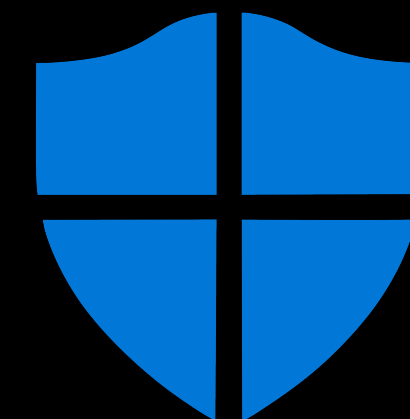
Hot Potato

Exploit WAPD



WPAD

HTTP Request for Update

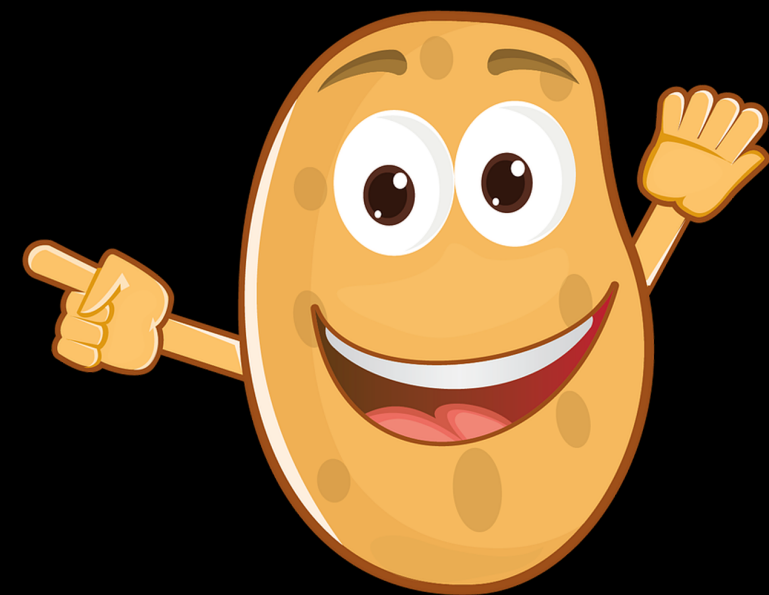


Windows Defender

# NTLM Reflection

---

Hot Potato - HTTP->SMB Reflection



Hot Potato

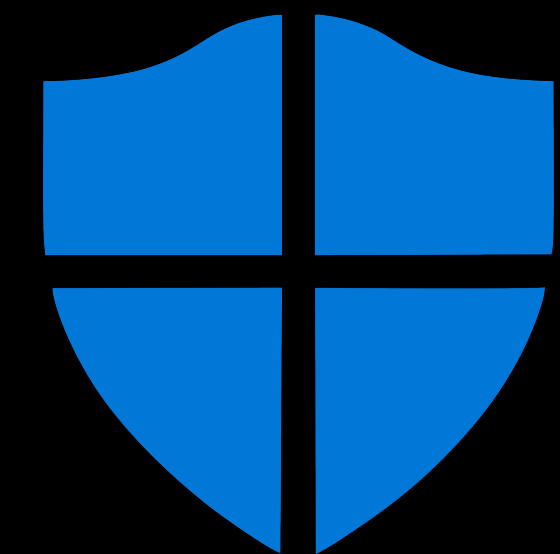
Send 401 HTTP Response



NTLM Authentication Automatically



System account

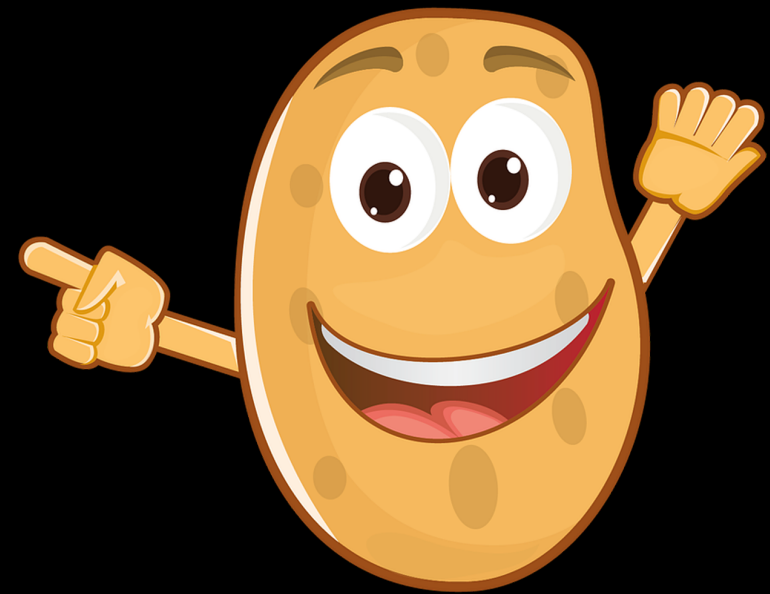


Windows Defender

# NTLM Reflection

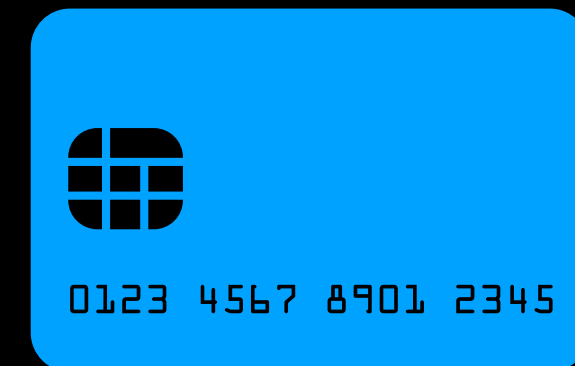
---

Hot Potato - HTTP->SMB Reflection



Hot Potato

Relay Net-NTLM hash to SMB Service



SMB Service



# NTLM Reflection

---

Hot Potato - HTTP->SMB Reflection

## ***MS16-075***

Fix local HTTP->SMB Reflection

## ***MS16-077***

WPAD Name Resolution will not use NetBIOS (CVE-2016-3213)

Does not send credential when requesting the PAC file(CVE-2016-3236)



# New technology to perform NTLM reflection attack



# NTLM Reflection

## A Journey to bypass MS16-075

### Unpatched

38	192.168.98.1	3.359475	192.168.98.146	TCP	54	80 → 49292 [ACK] Seq=358 Ack=537 Win=261824 Len=0
39	192.168.98.1	3.361675	192.168.98.146	SMB	236	Session Setup AndX Request, NTLMSSP_AUTH, User: \
40	192.168.98.146	3.362064	192.168.98.1	SMB	192	Session Setup AndX Response
41	192.168.98.1	3.362090	192.168.98.146	TCP	66	63611 → 445 [ACK] Seq=377 Ack=544 Win=131200 Len=0
42	192.168.98.1	3.362227	192.168.98.146	TCP	70	[TCP segment of a sequence established RST]
▼ SMB (Server Message Block Protocol)						
▼ SMB Header						
Server Component: SMB						
<a href="#">[Response to: 39]</a>						
[Time from request: 0.000389000 seconds]						
SMB Command: Session Setup AndX (0x73)						
NT Status: STATUS_SUCCESS (0x00000000)						
► Flags: 0x98, Request/Response, Canonicalized Pathnames, Case Sensitivity						
► Flags2: 0x4801, Error Code Type, Extended Security Negotiation, Long Names Allowed						





# NTLM Reflection

## A Journey to bypass MS16-075

Patched

26	192.168.98.1	0.225838	192.168.98.151	SMB	221	Session Setup AndX Request, NTLMSSP_NEGOTIATE
27	192.168.98.151	0.226159	192.168.98.1	SMB	352	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_
34	192.168.98.1	0.443404	192.168.98.151	SMB	236	Session Setup AndX Request, NTLMSSP_AUTH, User: \
35	192.168.98.151	0.443875	192.168.98.1	SMB	105	Session Setup AndX Response, Error: STATUS_ACCESS_DENIED
38	192.168.98.1	0.543386	192.168.98.151	SMB	142	Tree Connect AndX Request, Path: \\192.168.98.151\IPC\$
39	192.168.98.151	0.543593	192.168.98.1	SMB	105	Tree Connect AndX Response, Error: Bad userid

▶ Frame 35: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0

▶ Ethernet II, Src: Vmware\_11:47:69 (00:0c:29:11:47:69), Dst: Vmware\_c0:00:08 (00:50:56:c0:00:08)

▶ Internet Protocol Version 4, Src: 192.168.98.151, Dst: 192.168.98.1

▶ Transmission Control Protocol, Src Port: 445, Dst Port: 64441, Seq: 418, Ack: 377, Len: 39

▶ NetBIOS Session Service

▼ SMB (Server Message Block Protocol)

▼ SMB Header

Server Component: SMB

[\[Response to: 34\]](#)

[Time from request: 0.000471000 seconds]

SMB Command: Session Setup AndX (0x73)

NT Status: STATUS\_ACCESS\_DENIED (0xc0000022)

▶ Flags: 0x98, Request/Response, Canonicalized Pathnames, Case Sensitivity

▶ Flags2: 0x4801, Error Code Type, Extended Security Negotiation, Long Names Allowed

Process ID High: 0



# NTLM Reflection

---

A Journey to bypass MS16-075

## Flags in Type 2 Message

Contained in a bitfield within the header

Most of these will make **more sense late**

Description	Content
Signature	Null-terminated ASCII "NTLMSSP"
Message Type	long (0x02000000)
Target Name	the name of the authentication target
Flags	long
Challenge	8 bytes information about the authentication target
Context	8 bytes
Target Information	security buffer
Version	8 bytes



# Fuzzing NTLM Message Flags



# NTLM Reflection

A Journey to bypass MS16-075

*Get a different Type 3 Message!*

34	192.168.98.1	6.865052	192.168.98.151	HTTP	503	HTTP/1.1 401 Unauthorized , NTLMSSP_CHALLENGE (text/html)
35	192.168.98.151	6.869463	192.168.98.1	HTTP	734	GET /mkmMLvT3ILii5V HTTP/1.1 , NTLMSSP_AUTH, User: WIN77\Administrator
36	192.168.98.1	6.869538	192.168.98.151	TCP	54	8080 → 49261 [ACK] Seq=450 Ack=937 Win=261440 Len=0
▼ Negotiate Flags: 0x028a0205, Negotiate Version, Negotiate Target Info, Negotiate Extended Security, Target Type Server, Negotiate NTLM key, Request Target, Negotiate UNICODE						
0...	.....	.....	.....	.....	.....	= Negotiate 56: Not set
.0..	.....	.....	.....	.....	.....	= Negotiate Key Exchange: Not set
..0.	.....	.....	.....	.....	.....	= Negotiate 128: Not set
...0	.....	.....	.....	.....	.....	= Negotiate 0x10000000: Not set
....0...	.....	.....	.....	.....	.....	= Negotiate 0x08000000: Not set
.....0..	.....	.....	.....	.....	.....	= Negotiate 0x04000000: Not set
.....1.	.....	.....	.....	.....	.....	= Negotiate Version: Set
.....0	.....	.....	.....	.....	.....	= Negotiate 0x01000000: Not set
.....1...	.....	.....	.....	.....	.....	= Negotiate Target Info: Set
.....0...	.....	.....	.....	.....	.....	= Request Non-NT Session: Not set
.....0.	.....	.....	.....	.....	.....	= Negotiate 0x00200000: Not set
.....0	.....	.....	.....	.....	.....	= Negotiate Identify: Not set
.....1...	.....	.....	.....	.....	.....	= Negotiate Extended Security: Set
.....0..	.....	.....	.....	.....	.....	= Target Type Share: Not set
.....1.	.....	.....	.....	.....	.....	= Target Type Server: Set
.....0	.....	.....	.....	.....	.....	= Target Type Domain: Not set
.....0	.....	.....	.....	.....	.....	= Negotiate Always Sign: Not set
.....0..	.....	.....	.....	.....	.....	= Negotiate 0x00004000: Not set
.....0	.....	.....	.....	.....	.....	= Negotiate OEM Domain Supplied: Not set
.....0...	.....	.....	.....	.....	.....	= Negotiate Anonymous: Not set
.....0..	.....	.....	.....	.....	.....	= Negotiate NT Only: Not set
.....1.	.....	.....	.....	.....	.....	= Negotiate NTLM key: Set
.....0	.....	.....	.....	.....	.....	= Negotiate 0x00000100: Not set
.....0...	.....	.....	.....	.....	.....	= Negotiate Lan Manager Key: Not set
.....0..	.....	.....	.....	.....	.....	= Negotiate Datagram: Not set
.....0.	.....	.....	.....	.....	.....	= Negotiate Seal: Not set
.....0	.....	.....	.....	.....	.....	= Negotiate Sign: Not set



# NTLM Reflection

A Journey to bypass MS16-075

## Negotiate Local Call:

The server sets this flag to inform the client that the server and client are on **the same machine**

```
▼ Negotiate Flags: 0xa28ac205, Negotiate 56, Negotiate 128, Negotiate Version, Negotiate Target Info,
1... .. = Negotiate 56: Set
.0.. .. = Negotiate Key Exchange: Not set
..1. .. = Negotiate 128: Set
...0 .. = Negotiate 0x10000000: Not set
....0... = Negotiate 0x08000000: Not set
.... .0.. = Negotiate 0x04000000: Not set
.... ..1. = Negotiate Version: Set
.... ...0 = Negotiate 0x01000000: Not set
.... ....1... = Negotiate Target Info: Set
.... .....0.. = Request Non-NT Session: Not set
.... .... ..0. = Negotiate 0x00200000: Not set
.... .....0 = Negotiate Identify: Not set
.... .... 1... = Negotiate Extended Security: Set
.... .....0.. = Target Type Share: Not set
.... .... ..1. = Target Type Server: Set
.... .....0 = Target Type Domain: Not set
.... .....0 = Negotiate 0x00004000: Set
.... .....0 = Negotiate OEM Workstation Supplied: Not set
.... .... ..0 = Negotiate OEM Domain Supplied: Not set
.... .....0... = Negotiate Anonymous: Not set
.... .... ..0.. = Negotiate NT Only: Not set
.... .... ....1. = Negotiate NTLM key: Set
.... .... ...0 = Negotiate 0x00000100: Not set
.... .....0... = Negotiate Lan Manager Key: Not set
.... .... ..0.. = Negotiate Datagram: Not set
.... .... ...0. = Negotiate Seal: Not set
.... .....0 = Negotiate Sign: Not set
.... .... 0... = Request 0x00000008: Not set
.... .... .1.. = Request Target: Set
.... .... ..0. = Negotiate OEM: Not set
.... .... ...1 = Negotiate UNICODE: Set
NTLM Server Challenge: d2bc662dc82faafc
Reserved: 303c460100000000
```

# NTLM Reflection

---

A Journey to bypass MS16-075

***VIDEO DEMO***



# NTLM Reflection

---

A Journey to bypass MS16-075

*Now we bypass Microsoft patch successfully!*





# Rebirth Hot Potato

HTTP->SMB NTLM Reflection&WAPD Attack



# NTLM Reflection

---

Potato Rebirth - Bypass MS16-075

- **MS16-075**
  - Fix local HTTP->SMB Relay
  - Windows Defender Update Client will send a Net-NTLM hash that can't be exploited



# NTLM Reflection

---

Potato Rebirth - Bypass MS16-075

<http://go.microsoft.com/fwlink/?LinkID=121721>





\_\_\_\_\_

## ot TLRMTUNTUAAADAAAAGAAAYAIYAAADkAOQAngAAAAoACgBYAAAAAGgAaAGIAAAAKAAoAfAAAAAAAAAA

The image shows two screenshots from a Windows 10 environment. The top screenshot is a File Explorer window displaying the contents of the 'Program Files (x86)' directory. A file named 'pwned' is selected, and its properties are shown at the bottom: 'pwned' (文件), '修改日期: 2019/3/16 14:47', '创建日期: 2019/3/16 9:20', and '大小: 0 字节'. The bottom screenshot shows the 'Windows 更新历史记录' (Windows Update History) window. It displays a table of updates with the following data:

名称	状态	重要性	安装日期
Windows 安全更新程序 (KB3161561)	成功	重要	2019/3/14



# NTLM Reflection

---

Potato Rebirth - MS16-077

***MS16-077:***

WPAD Name Resolution will not use NetBIOS (CVE-2016-3213)

Does not send credential when requesting the PAC file(CVE-2016-3236)

**WAPD MITM Attack is Dead!**



# NTLM Reflection

---

Potato Rebirth - MS16-077

## ***Compromising IPv4 networks via IPv6***

using mitm6 to abuses the default IPv6 configuration in Windows network to spoof DNS replies by acting as a malicious DNS server and redirect traffic to an attacker-specified endpoint.

**WAPD MITM Attack Rebirth!**



# NTLM Reflection

---

Potato Rebirth - MS16-077

***Combined 3 vulnerabilities to perform Privilege Escalation***

1. Compromising IPv4 networks via IPv6 to hijack WAPD
2. Use [go.microsoft.com](https://go.microsoft.com) to get an authentication
3. Change flag in NTLM Type 2 Message to bypass MS 16-75

**Hot Potato Rebirth!**



# Incidentally

---

***Man-in-the-middle Attack are required before most NTLM attacks***

- Poison DNS
- Spoof NetBIOS/LLMNR
- ARP attack
- Exploit the WPAD
- etc

**We always relay to SMB.**

**We need to wait and wait.**



# A Whole New perspective In SSRF

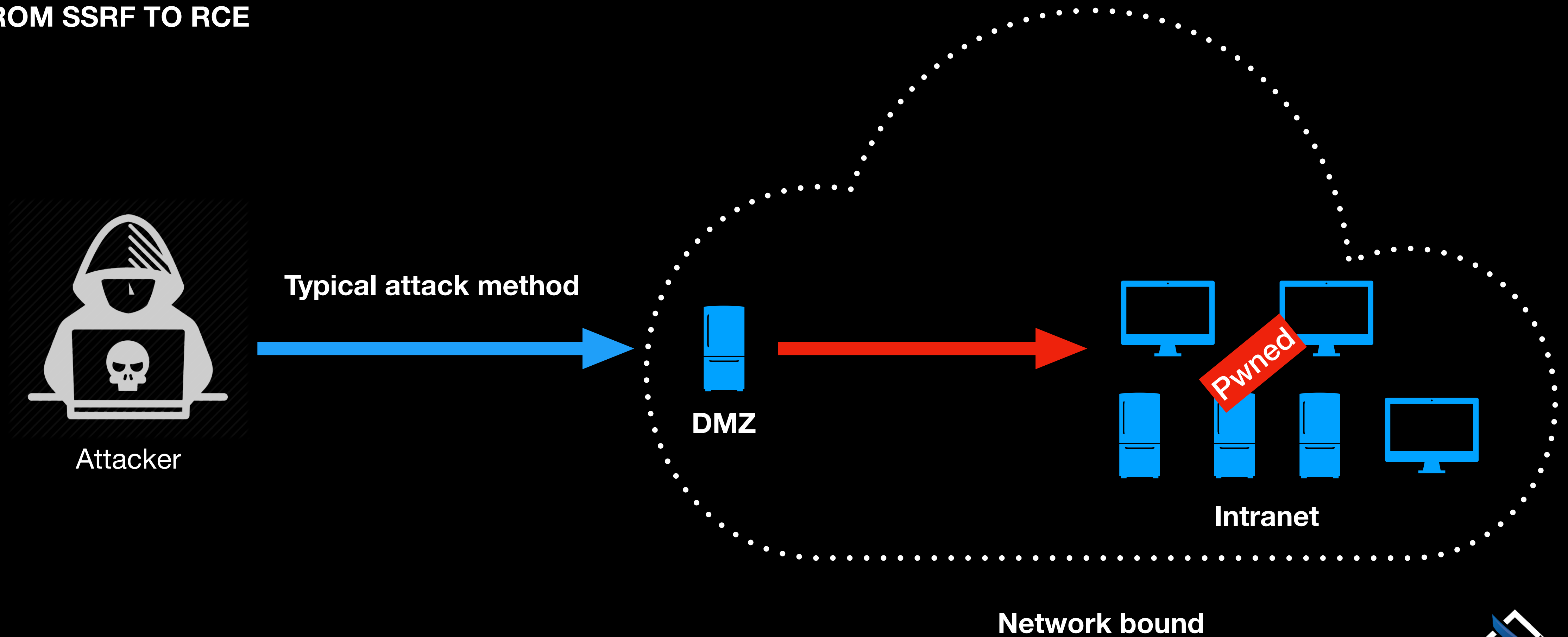
Ignore Many SSRF defense&Directly lead to RCE Via once exploit





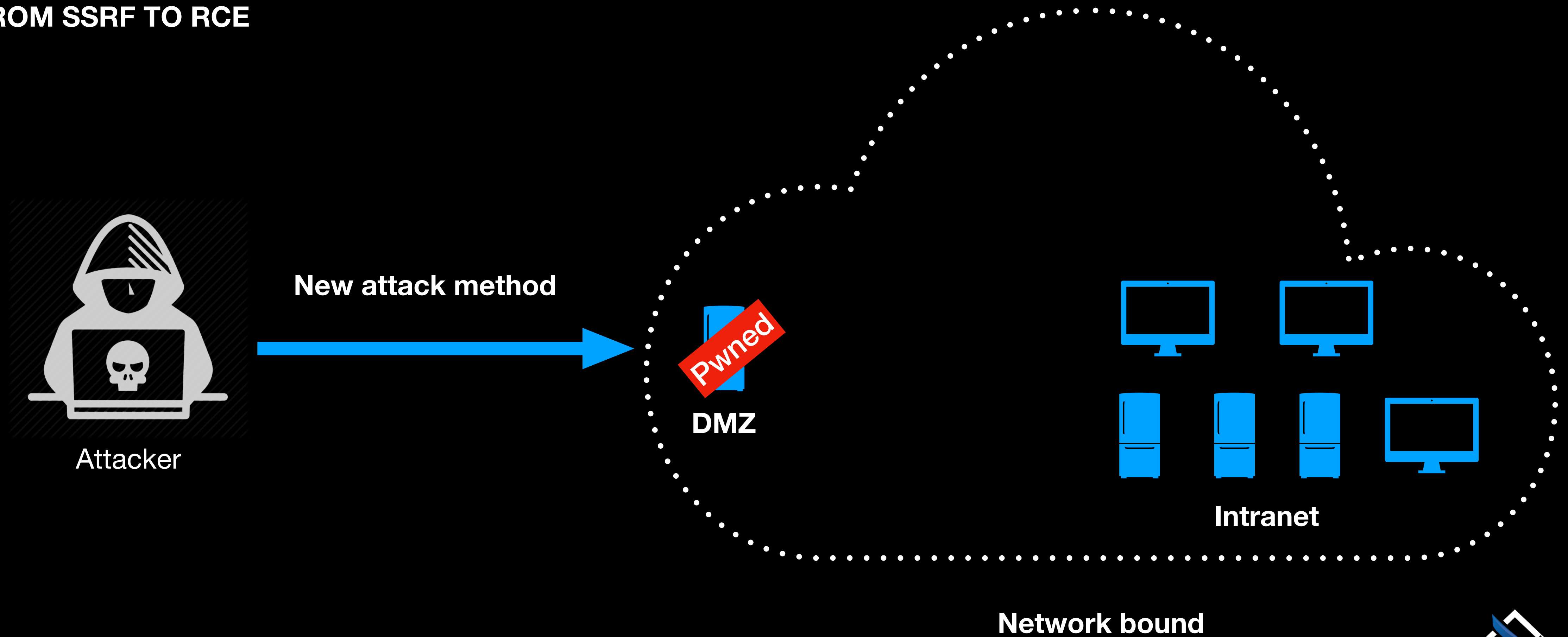
# New perspective In SSRF

FROM SSRF TO RCE



# New perspective In SSRF

FROM SSRF TO RCE





# New perspective In SSRF

---

## FROM SSRF TO RCE

### Attack Network Connector

- Completely ignore most of the SSRF defense solutions.
- Once exploiting can directly lead to the impact of RCE.
- Increasing the risk of many SSRF vulnerabilities which have been considered in low impact.



# Critical Security Issue in JAVA



# Critical Security Issue

---

**FROM SSRF TO RCE**

## **URLConnection**

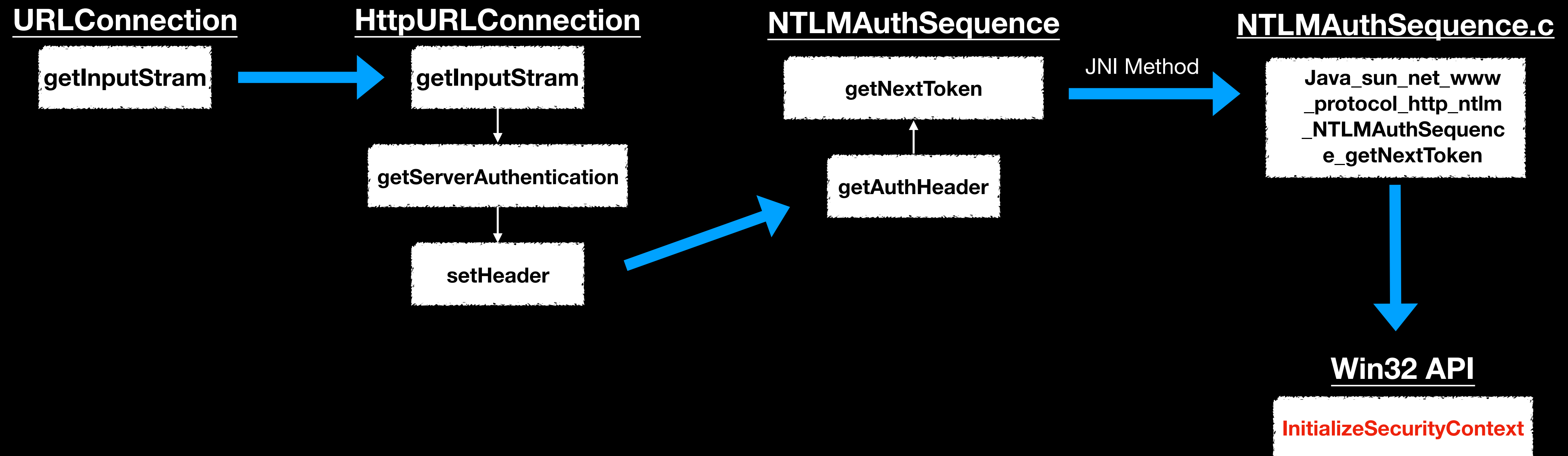
The superclass of all classes that represent a communications link between the application and a URL.

The most of JAVA function use URLConnection to send HTTP request.



# Critical Security Issue

## FROM SSRF TO RCE



# Critical Security Issue

---

## FROM SSRF TO RCE

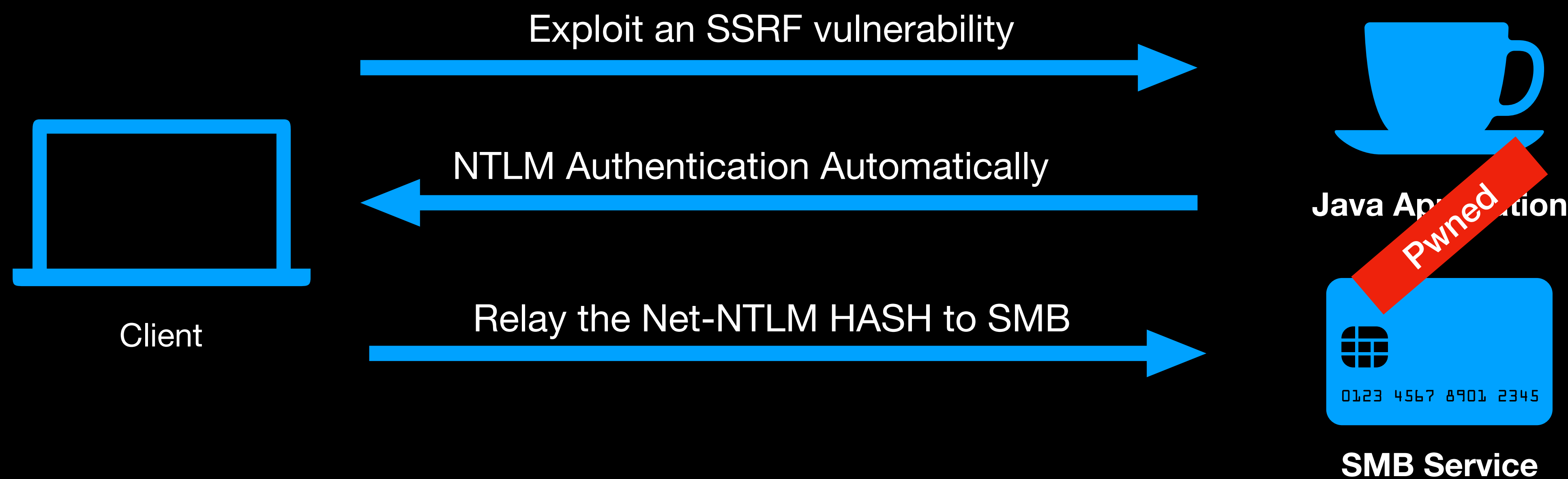
**The default behavior of Java will not judge the validity of the URL,  
but always return true.**

```
static class DefaultNTLMAuthenticationCallback extends NTLMAuthenticationCallback{  
  
    DefaultNTLMAuthenticationCallback() {  
  
        public boolean isTrustedSite(URL var1) {  
            return true;  
        }  
    }  
}
```



# Critical Security Issue

## FROM SSRF TO RCE



# Critical Security Issue

---

FROM SSRF TO RCE

***VIDEO DEMO***



# NTLM Reflection

---

FROM SSRF TO RCE

**Affects all JDK versions!**





# NTLM Reflection

---

FROM SSRF TO RCE

**An SSRF vulnerability is required, is that all?**



# The new era in NTLM Reflection



# NTLM Reflection

---

New era in NTLM Reflection

## **NTLM Authenticate Automatically**

Security issue in Java basic Class, that means most of JAVA application is affected.

## **Influence Expansion**

Not just SSRF, anything which will send an HTTP request to us is affected.  
Over other vulnerabilities, such as XXE, Deserialization, etc.



# Java Deserialization



# NTLM Reflection

---

## New era in NTLM Reflection

### **Deserialization Attack (Affects most of Java application)**

Chris Frohoff and Gabriel Lawrence presented their research into Java object deserialization vulnerabilities ultimately resulting in what can be readily described as the biggest wave of RCE bugs in Java history.

After two years later, Moritz Bechler releases a tool to achieve code execution during the unmarshalling process in 2017.

### **How to fixed?**

Add a blacklist to mitigate Java Deserialization Attack.



# NTLM Reflection

---

New era in NTLM Reflection

## **Bypass all Java Deserialization Blacklist**

Just need to find a gadget that will send an HTTP request to us.

## **Affected Software**

All Java applications use a class blacklist to mitigate deserialization attack are affected.



# Bypass all Java Deserialization Blacklist

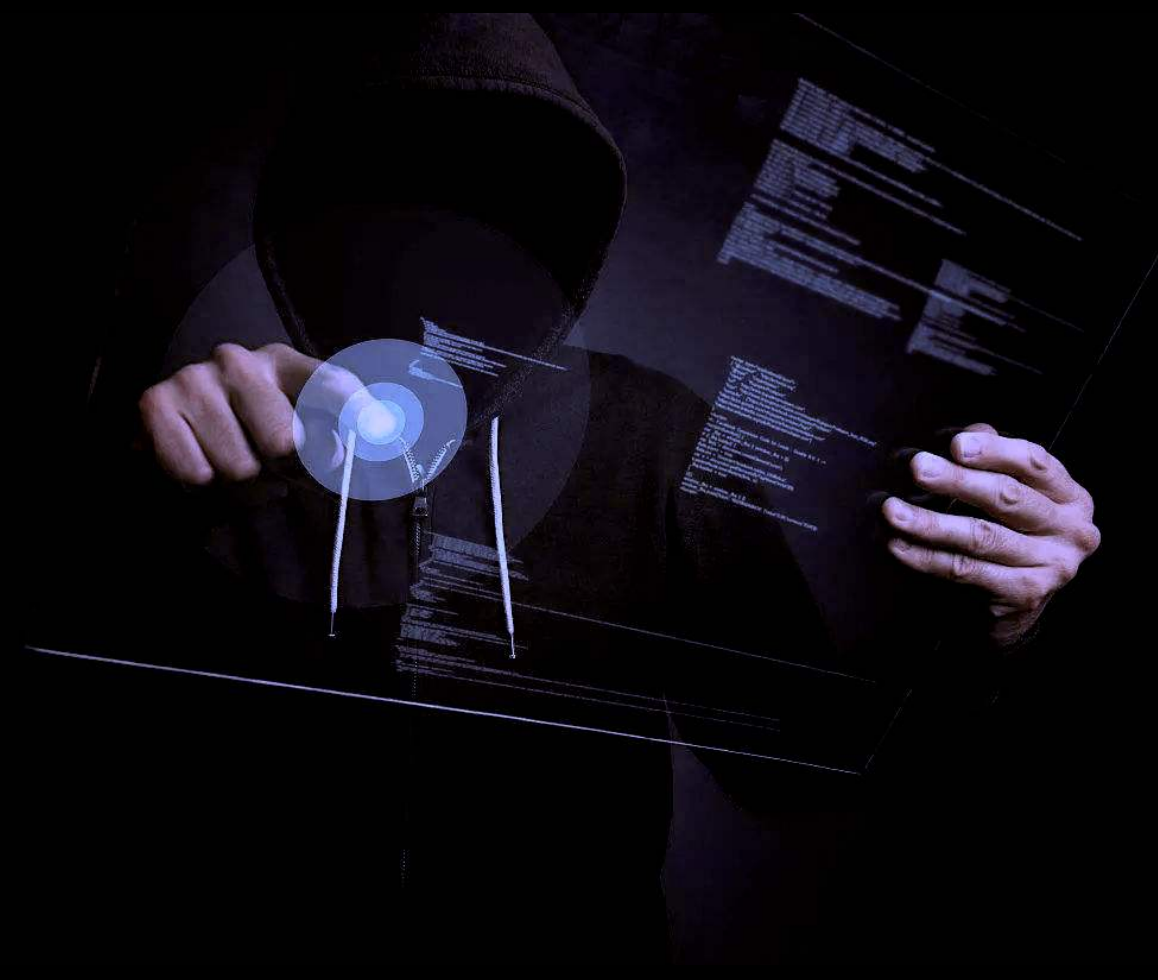
## Directly lead to RCE



# NTLM Reflection

## New era in NTLM Reflection

- ✓ SSRF
- ✓ Deserialization
- ✓ XXE
- ✓ Database
- ✓ Sandbox
- ✓ Java Security Scanner
- ✓ Java Crawler
- ✓ Cloud Service
- ✓ Man-In-The-Middle
- ✓ **Anything sends an HTTP request to us**



▶ HTTP

▶ SMTP

▶ LDAP

▶ etc...

**Pwned**





# Acknowledgement

---

- OPCDE
- Impacket (@SecureAuthCorp)
- Responder (@SpiderLabs)
- mitm6 (@Foxglove Security)
- ZackAttack(@Urbane Security)



# Thanks!

@by\_sanr - [ssssanr@gmail.com](mailto:ssssanr@gmail.com)

@izykw - [izykeepwalking@gmail.com](mailto:izykeepwalking@gmail.com)



Back2Zero