THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

ClickOnce-Based APT Malware Targeting Critical Infrastructure

CATEGORY

APT Malware

SEVERITY

Critical

Platforms

Windows

IMPACT

- Advanced Persistence and Evasion Techniques
- In-Memory Modular Payload Execution
- Abuse of Cloud Services for Command and Control
- Targeted Attacks on Critical Infrastructure
- Potential for State-Sponsored Espionage
- High Risk to Operational Continuity and Data Security

Description

ClickOnce-Based APT Malware Targeting Critical Infrastructure

Researchers have identified an active and sophisticated malware campaign known as 'OneClik.' The campaign leverages Microsoft ClickOnce deployment technology to deliver modular .NET malware, effectively bypassing standard security mechanisms. Technical indicators and tactics closely align with China-affiliated APT groups, though definitive attribution remains cautious

Technical Summary:

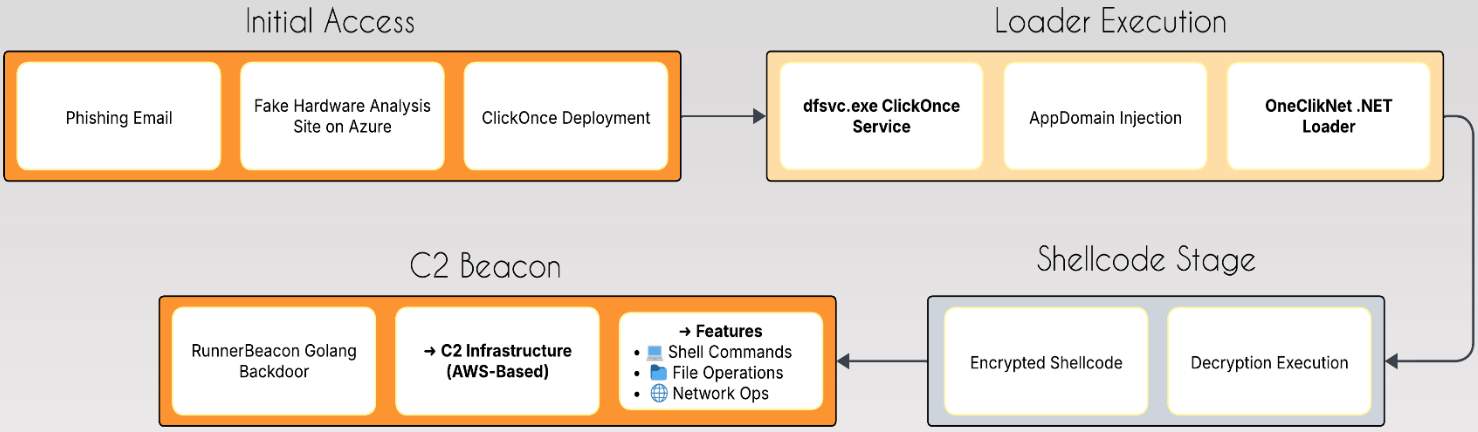
Technical Summary:

Initial Access: Victims receive phishing emails linking to fake hardware analysis sites that deliver a malicious ClickOnce manifest.

Execution: Malware runs via the trusted dfsvc.exe, using AppDomainManager hijacking (T1574.014) through .exe.config tampering to load DLLs into legit processes like ZSATray.exe.

Payload Delivery: A .NET stager (OneClikNet) collects system data and decrypts AES-encrypted, base64 payloads in memory using CLR reflection and shellcode injection, evading standard detections.

Infection chain and technical analysis



Initial Access

Phishing Email

Fake Hardware Analysis Site on Azure

ClickOnce Deployment

Loader Execution

dfsvc.exe ClickOnce Service

AppDomain Injection

OneClikNet .NET Loader

Shellcode Stage

Encrypted Shellcode

Decryption Execution

C2 Beacon

RunnerBeacon Golang Backdoor

→ C2 Infrastructure (AWS-Based)

→ Features

- 💻 Shell Commands
- 📁 File Operations
- 🌐 Network Ops

Indicator of Compromise

SHA-256

```
b06b1a5ea83d7f0883f9388c83359a738bc90e092f21f458232e2f98ed9810b6
bea96cbf485f32fff1cf5cd9106ada542b978094f524f052f0391c3b916846df
296030c3a5c7422884d0fda4fbcef7d6cbb227074719083369231597 7f7f3c7d
e61d6e88f1f0068288bb0df226b433915ae295f040475d85f0960f1db0b43ca8
4007350e16856cb9bb1fc1ca6e359e00b0776a5d1229f83f54e730e1d67ddbce
18f498b78b02050cbb80c75de035e1985adf8bc838665f0f8a22d3ed3304f73d
c045503e0cb85588097c6e2484a49c52251ed5e46e9bfc6c73574440534123c9
048ffb71a1e5abfd6b905b7a4a5171eabe560948963a8c0d6aa14a40d0f6b255
af8864bde7e2a3b6ff198939c8350c42cea51556b1bb8be6476650ae86c2e669
d830f27b1dfc75ac50f89a9353fd8aa90103e9a53562475ab69e12d5969b70b2
4272b9bfc559d60c967fc5e8d17a61ab33aea14522fbfda1341f3953d7d1fb19
403e7effd2ac31ebcf9181fb4851b309a4448079bd117a90d1e670ac235989de
0192212b4784ee4e483d162959daf89674cb98aaa6d065e1621a5d26e66a77f3
2a07875fca7a9c15aa54e82a91800899effadda919e5548513c13586f2c3d7fc
949c3c79877ce6e4963131e0888c3de4b256bac1de28601c6b01bbfcce7865e0
86f6d5ebaeb5ea5ac3b952e38951658e716f6065ce5f689ab5cf62fd738525e9
83f21a03db7cd2c621da3af0b40f6d39e2562af10b59cedfbc46868b054ffac7
0b61707d1fc8821a95c899de0304a55d549c7252ca24d5978f0989f9593a79c2
f2c6a9eed870d312be3b7c51998c5326fab17e999d0004931ff84b25233bc9b1
ea38f13b9ef3ce8351f64ad3685d5fa5fb35e507c71002560f12b24b8c8b546b
8facceb0b15bbf061ae9ebcb3b97980d90d774c035ece434e4653299afc7babc
b3dd3b9e8c999fe0e1273a52288af65e1f0997a587f3aa2f13e2a0e6f4383f22
```

Indicator of Compromise

MD5

2afcc359528893cc2649957c82200937

e355e138bd2e5179c75f1e382e8bbb05

33b2bfe7bd62c0ee00601083995729fb

e5a897f076c28d23c37c29bef57bc3a4

c9c36cafcf939e3b70609559d99c2e04

992d046808217492560285 8b426b7603

2cbdd1172f31ab41f1590d9499da8dcb

ae0401c1cccb1e8a606b3504268f1277

babf82a54aae4246678b5f16a15cb35f

deb7831bdf189610889fe033a63fd4e0

SHA-1

684c53a07ca0928f5bc4a31e15be7be6ca25b2bd

eee8b975bfb640ffb99a2d3065998b4edab704c8

8329dc43b776bf040aa646154016748b688d8ee9

034ec391503041836fcc1e0d8d52ecfeea41f8f1

eacb62b12852793552412e0cec7fd0fe17e58599

f205d2a3bc6e0551c6a9673c82836b89adc8e3eb

69c4087b7992fbaeb66c3a51a712dc66afbe1de4

5bd9b1698dc885ec18b6ad5e97ff6529815ae337

f70b2e8fe1bdea492bbec231c6ae0982c667ac16

d2609e8a7c65c33b6182936d6322625d8015c010

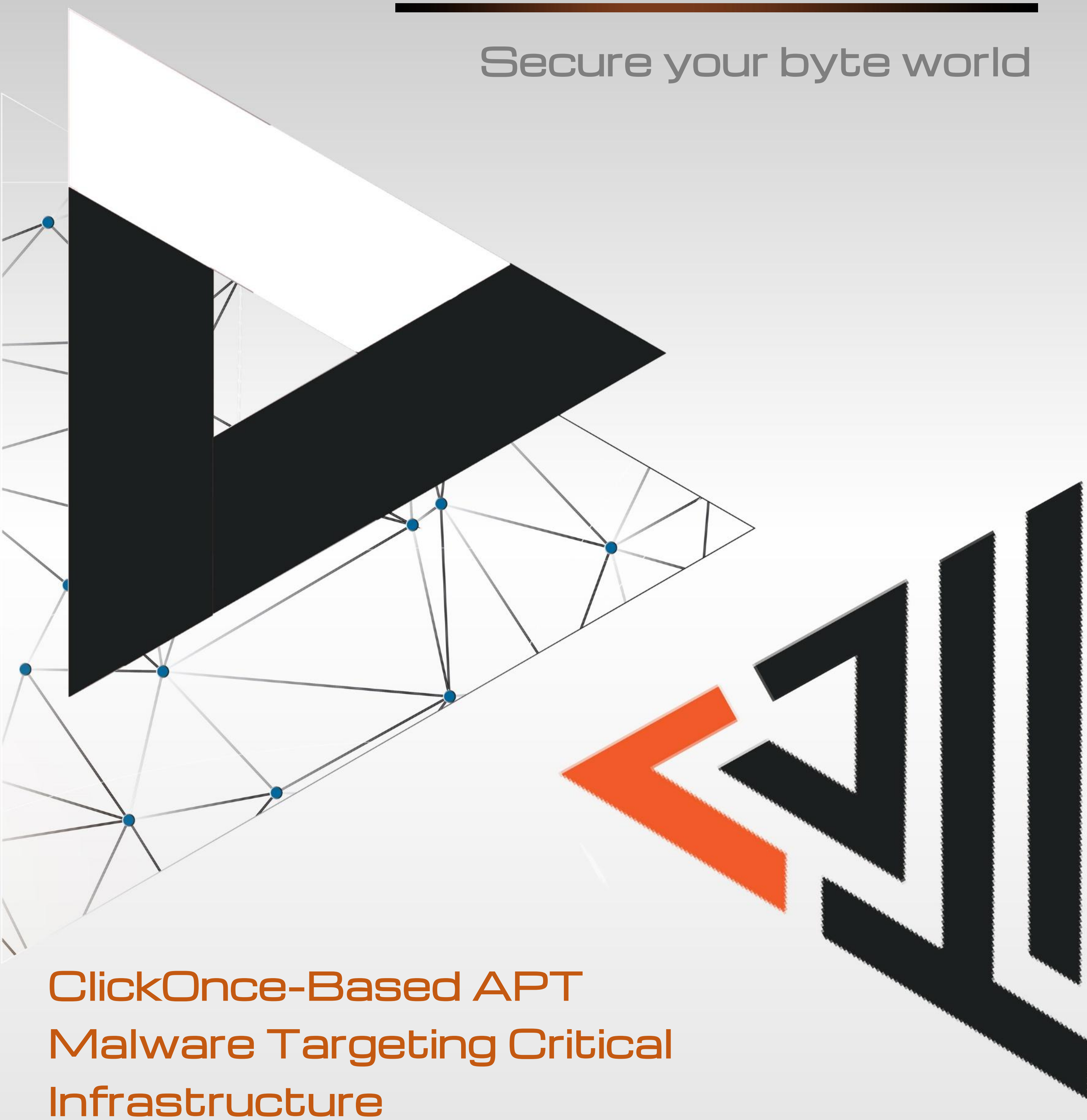
Recommended Immediate Actions

- Warn users about emails containing links to Azure blob storage or similar cloud-hosted lures.
- Implement application whitelisting to restrict unknown or unsigned .NET applications.
- Monitor executions of dfsvc.exe in unusual locations or with unexpected parameters.
- Set SIEM alerts for AppDomainManager hijacking (T1574.014) and .config file tampering.
- Enable .NET runtime logging (ETW) and integrate with EDR/SIEM solutions.
- Create incident response playbooks to handle memory-only malware and encrypted payloads.
- Educate users to identify phishing emails disguised as software analysis tools.
- Apply least privilege to user accounts to reduce post-exploitation impact.
- Patch vulnerable third-party applications commonly exploited for persistence (e.g., Adobe Reader, Flash).

ThreatCure

Cyber Threat Advisory

Secure your byte world



ClickOnce-Based APT Malware Targeting Critical Infrastructure

Get Started Today

For more information about the ThreatCure ShieldOps Platform or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE