Cyber Threat Advisory

Tick

Threat Actor Malware

CATEGORY

Malware

SEVERITY

High

Platforms

Windows & Linux

IMPACT

- Data Theft and Espionage
- National Security Implications
- Economic Consequences
- Supply Chain Risks
- Reputation Damage
- Mitigation Efforts

Description

Tick

Tick has globally impacted seven countries. The advanced persistent threat group known as 'Tick' has been conducting cyber espionage campaigns targeting organizations in the Republic of Korea and Japan over an extended period. Their primary focus is on companies possessing intellectual property or sensitive information, particularly those in the Defense and High-Tech sectors. Tick employs a combination of custom malware, such as Daserf, Invader, 9002, Minzen, NamelessHdoor, Gh0stRAT Downloader, Custom Gh0st, Datper, and HomamDownloader, alongside various commodity and bespoke tools. They exploit vulnerabilities and employ social engineering tactics.

Tick previously used domains registered through privacy protection services to keep their anonymity, but have moved to compromised websites in recent attacks. With multiple tools and anonymous infrastructure, they are running longstanding and persistent attack campaigns. We have observed that the adversary has repeatedly attacked a high-profile target in Japan using multiple malware families for the last three years.

Indicator of compromise

SHA-256

04080fbab754dbf0c7529f8bbe661afef9c2cba74e3797428538ed5c243d705a

f8458a0711653071bf59a3153293771a6fb5d1de9af7ea814de58f473cba9d06

e8edde4519763bb6669ba99e33b4803a7655805b8c3475b49af0a49913577e51

21111136d523970e27833dd2db15d7c50803d8f6f4f377d4d9602ba9fbd355cd

9c7a34390e92d4551c26a3feb5b181757b3309995acd1f92e0f63f888aa89423

0df20ccd074b722d5fe1358b329c7bdebcd7e3902a1ca4ca8d5a98cc5ce4c287

e9574627349aeb7dd7f5b9f9c5ede7faa06511d7fdf98804526ca1b2e7ce127e

57e1d3122e6dc88d9eb2989f081de88a0e6864e767281d509ff58834928895fb

933d66b43b3ce9a572ee3127b255b4baf69d6fdd7cb24da609b52ee277baa76e

2bec20540d200758a223a7e8f7b2f98cd4949e106c1907d3f194216208c5b2fe

797d9c00022eaa2f86ddc9374f60d7ad92128ca07204b3e2fe791c08da9ce2b1

9374040a9e2f47f7037edaac19f21ff1ef6a999ff98c306504f89a37196074a2

26727d139b593486237b975e7bdf93a8148c52d5fb48d5fe540a634a16a6ba82

dfc8a6da93481e9dab767c8b42e2ffbcd08fb813123c91b723a6e6d70196636f

ce47e7827da145823a6f2b755975d1d2f5eda045b4c542c9b9d05544f3a9b974

e34f4a9c598ad3bb243cb39969fb9509427ff9c08e63e8811ad26b72af046f0c

8e5a0a5f733f62712b840e7f5051a2bd68508ea207e582a190c8947a06e26f40

7d70d659c421b50604ce3e0a1bf423ab7e54b9df361360933bac3bb852a31849

a624d2cd6dee3b6150df3ca61ee0f992e2d6b08b3107f5b00f8bf8bcfe07ebe7

055fe8002de293401852310ae76cb730c570f2037c3c832a52a79b70e2cb7831

Domain Name

lywjrea.gmarketshop.net

krjregh.sacreeflame.com

psfir.sacreeflame.com

lywja.healthsvsolu.com

phot.healthsvsolu.com

blog.softfix.co.kr

news.softfix.co.kr

www.gokickes.com

log.gokickes.com

sansei.jpn.com

lywjrea.gmarketshop.net

krjregh.sacreeflame.com

psfir.sacreeflame.com

lywja.healthsvsolu.com

phot.healthsvsolu.com

blog.softfix.co.kr

news.softfix.co.kr

www.gokickes.com

log.gokickes.com

sansei.jpn.com

Remediation

- Patch & Update: Keep everything updated (OS, software)
- Software Management: Install from trusted sources, remove unused programs.
- Strong Auth: Use strong passwords and enable two-factor authentication (2FA).
- Educate Users: Train staff on cyber threats and encourage reporting suspicious activity.
- Network Security: Utilize firewalls and intrusion detection/prevention systems (IDS/IPS).
- Endpoint Security: Install antivirus/anti-malware and consider advanced endpoint protection.
- Backup & Recover: Regularly backup data and develop a disaster recovery plan.
- Prepare to Respond: Have an incident response plan and test it regularly.
- Stay Informed: Keep up-to-date on cyber threats and vulnerabilities.
- Block all IOCs on your XDR, EDR and other security tools.

THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

Cyber Threat Advisory

Secure your byte world

+1 (832) 271 2738

info@threatcure.net

https://threatcure.net/