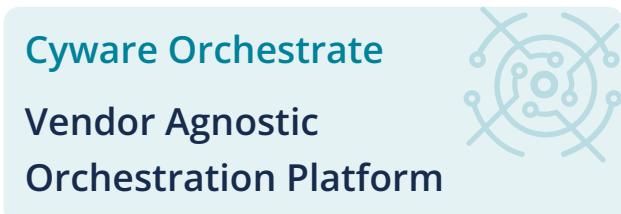
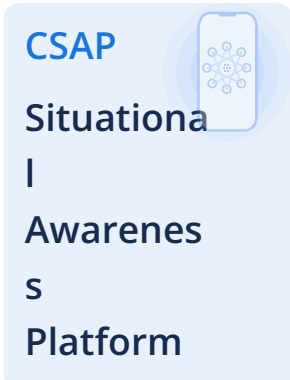
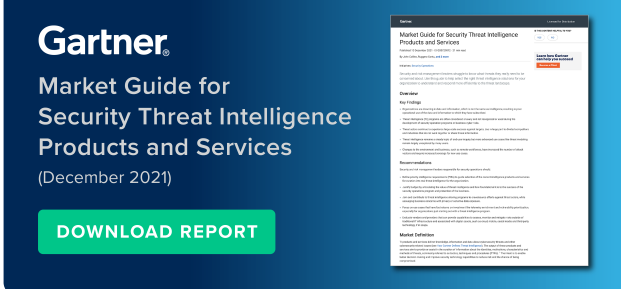


Go to listing page

GandCrab creator PINCHY SPIDER and its affiliates update tactics to spread the ransomware

Malware and Vulnerabilities

March 07, 2019 • Cyware Hacker News



- PINCHY SPIDER, the creator of GandCrab, and its affiliates were observed targeting the ransomware at enterprise environments.
- The group is also believed to be offering their share of profits to other entities spreading GandCrab.

GandCrab ransomware which made news last year has resurfaced again with new tactics and techniques. Cybersecurity firm CrowdStrike has detailed the ransomware’s recent activity in its latest blog.

According to the firm, the creator PINCHY SPIDER and its affiliates were found using techniques mainly associated with penetration testing teams as well as other adversary groups.

The big picture

- PINCHY SPIDER is now seen targeting enterprise environments with lateral movement techniques.
- Enterprise components include the popular IT systems management software LANDesk, used by many companies.
- Two affiliate threat groups labeled as ‘23’ and ‘110’ were detected by CrowdStrike in the ransomware campaign.
- PINCHY SPIDER also accepted ransom payments on a per-host basis, instead of the regular one-time payments for decryption.
- On the other hand, the group is also reportedly sharing profits from its campaigns with other groups or affiliates for spreading the ransomware.
- In February, the group released GandCrab 5.2 which had major improvements over the previous versions.

“Big Game Hunting” tactics - CrowdStrike pointed out that the group’s new tactics may be part of a strategy to cripple large corporate networks.

“The change in deployment tactics observed in these recent incidents, coupled with PINCHY SPIDER’s advertising for individuals with skills in RDP/VNC and experience in corporate networking, suggest PINCHY SPIDER and their affiliates are expanding to adopt big game hunting tactics,” CrowdStrike researchers wrote in the [blog](#).

The group was also seen aggressively advertising to find people with Remote Desktop Protocol (RDP) and Virtual Network Computing (VNC) skills to perpetrate large-scale ransomware attacks.

PINCHY SPIDER

Lateral Movement Techniques

Big Game Hunting

GandCrab v5

GandCrab ransomware



PREVIOUS

Unpatched UPnP-enabled devices allow attackers to take ...

Malware and Vulnerabilities



NEXT

Whitefly threat actor group linked to the massive Singh ...

Threat Actors

CATEGORIES

Expert Blogs and Opinion

Strategy and Planning

Cyber Glossary

Social Media Threats

EVENTS

Conference

Innovation and Research

Mobile Security

Threat Actors

Security Tips and Advice

Webinar

The Hacker Tools

Govt., Critical

Security Products & Services

Interesting Tweets

Summit

Incident Response, Learnings

Infrastructure Identity Theft, Fraud, Scams

Threat Intel & Info Sharing

Marketplace

Course

Malware and Vulnerabilities

Security Culture

Emerging Threats

Did You Know?

Symposium

Breaches and Incidents

Trends, Reports, Analysis Geopolitical, Terrorism

Physical Security

Talk

Laws, Policy, Regulations

New Cyber Technologies Internet-of-Things

Seminar

Companies to Watch

Major Events

Computer, Internet Security

Others

News and Updates, Hacker News

Get in touch with us now!

1-855-692-9927



Download Cyware Social App



Terms of Use

Privacy

Policy

© 2022