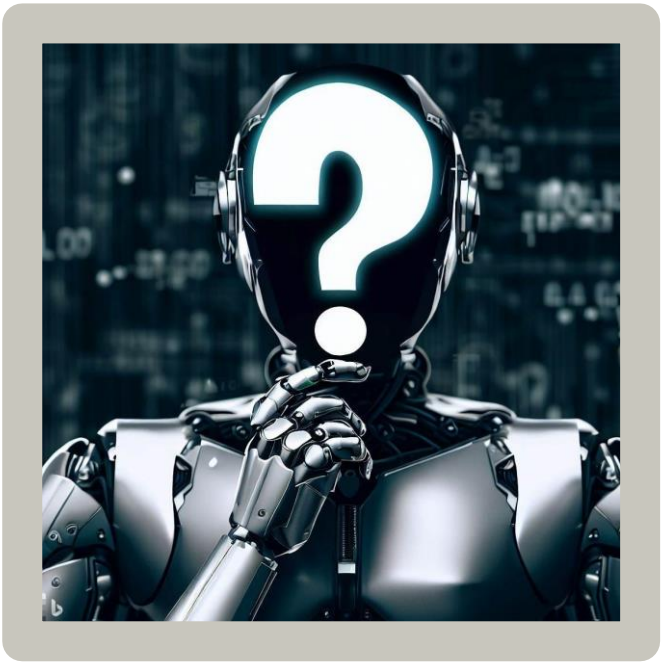

[Actor Preview]

Code Name:
Nosferatu Campaign

Affiliation(s):
No known affiliations. Likely independent financially motivated group.

Operating Region(s):
Likely operating across multiple regions using anonymized infrastructure.

Motivation(s): Financial gain and intellectual property theft (Krabby Patty formula).

Summary: The Nosferatu Campaign is a phishing-based operation targeting employees of the Krusty Krab. The threat actor used multiple email accounts and malicious domains to harvest credentials, compromise accounts, and exfiltrate sensitive files. They relied heavily on spearphishing emails with malicious links and attachments to deploy malware such as krabbypatty.exe, enabling persistence and data theft.

Initial Access Vector

The threat actor sent spearphishing emails from accounts such as nosferatu.hash@hotmail.com and nosferatu@gmail.com. Emails contained malicious links hosted on domains like scarynight.net and sleeve-dark.net, which redirected to credential harvesting pages. Employees including Julie Hong and Toni Jones clicked these links, leading to credential compromise.

Post Exploitation Activity

After gaining initial access, the actor logged into compromised accounts, including Tina Morrow and Hector Duncan. They performed reconnaissance on the Krusty Krab website, searching for job listings and sensitive information. The actor downloaded files from employee mailboxes, such as important.zip and email.7z. Malicious attachments (Jellyfish_Guide.pptx, Free_Money.pdf, Secret_Formula.docx) deployed krabbypatty.exe and DLL files, providing privilege escalation and persistence across multiple hosts.

Command and Control

The actor established C2 communication using PowerShell commands and malware callbacks. krabbypatty.exe injected DLLs (CX3VBWML.dll, CW8VCRZ1.dll) that communicated with IPs such as 59.240.32.173 and 213.173.220.223. Over 28 systems executed similar PowerShell commands to connect to external servers.

Exfiltration and Impact

The actor staged sensitive files into local directories before exfiltrating them. They used rclone.exe to transfer data to domains like computer-wifesecret.com. Email archives and deleted mails were stolen. In total, 26 systems were compromised, and critical data including employee communications and potentially the Krabby Patty recipe was at risk.

Appendix: Indicators of Compromise

Domains:
- scarynight.net
- sleeve-dark.net
- night-shift.com
- midnighttech.dev
- burgers-formula.biz
- chumsecret.biz

Threat IPs:
- 54.17.157.246
- 136.61.241.165
- 50.6.66.245
- 59.240.32.173
- 213.173.220.223

Malicious Files:
- Jellyfish_Guide.pptx
- Free_Money.pdf
- Secret_Formula.docx
- krabbypatty.exe
- CX3VBWML.dll
- CW8VCRZ1.dll

Emails:
- nosferatu.hash@hotmail.com
- nosferatu@gmail.com
- graveyard@hotmail.com
- slasher.graveyard@hotmail.com
- legal.human_resources@yandex.com
- legal.vendor@protonmail.com
- payroll.human_resources@aol.com

Analyst Notes

The Nosferatu Campaign demonstrates how persistent phishing combined with poor user awareness can lead to widespread compromise. The actor relied heavily on credential theft and email-based attacks to escalate access. Effective security awareness training, email filtering, and stronger authentication mechanisms could have mitigated much of this activity.