SOC141 - Phishing URL Detected

Caso conduzido individualmente no simulador SOC da plataforma LetsDefend. Atuei como analista SOC N1, realizando todas as etapas de triagem, investigação, contenção e relatório.

📝 Descrição:

Recebido o alerta SOC141, sinalizando que o host EmilyComp (172.16.17.49) acessou uma URL maliciosa de phishing no domínio mogagrocol.ru. A conexão foi permitida, sendo necessária uma investigação mais aprofundada.

🧠 Análise:

Em 22 de março de 2021, às 21h23, o alerta foi gerado indicando que a URL acessada:

hxxp://mogagrocol.ru/wp-content/plugins/akismet/fv/index.php?email=ellie@letsdefend.io

poderia estar associada a conteúdo malicioso. O domínio mogagrocol.ru possui origem na Rússia, o que já levantou uma suspeita adicional.

A análise detalhada revelou:
- O domínio executou um comando malicioso via rundll32.exe, carregando um script HTML/JavaScript.
- O script tentava baixar e executar o malware KBDYAK.exe a partir da URL: hxxp://ru-uid-507352920.pp.ru/KBDYAK.exe

🛠️ Ação tomada:

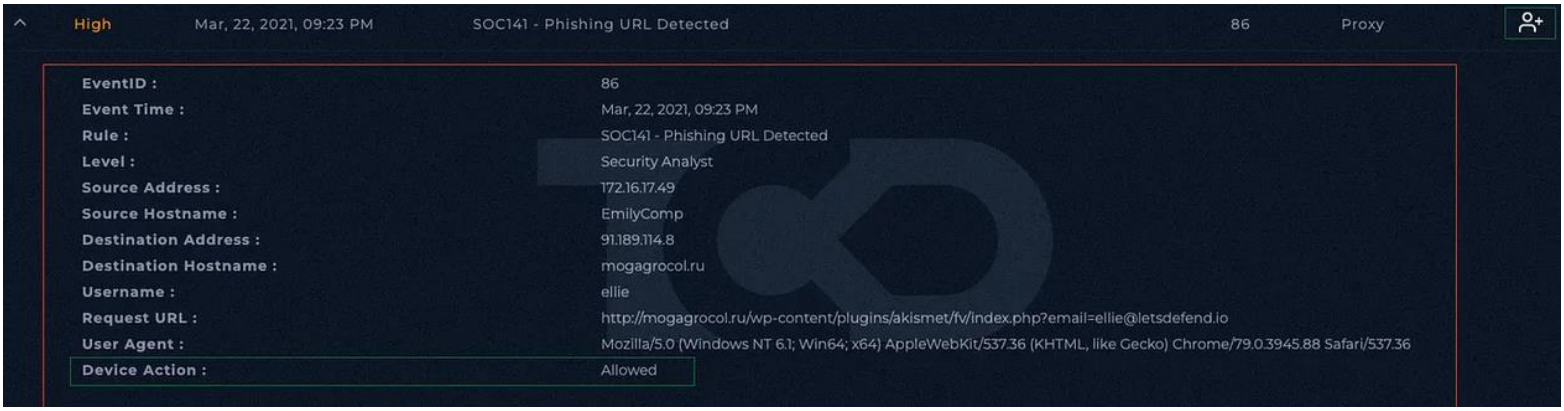
- O alerta foi classificado como **True Positive** após validações de reputação do domínio, execução do script malicioso e análise comportamental.
- O host EmilyComp (172.16.17.49) foi imediatamente isolado via EDR (conforme Playbook) para conter o risco de movimentação lateral ou persistência.

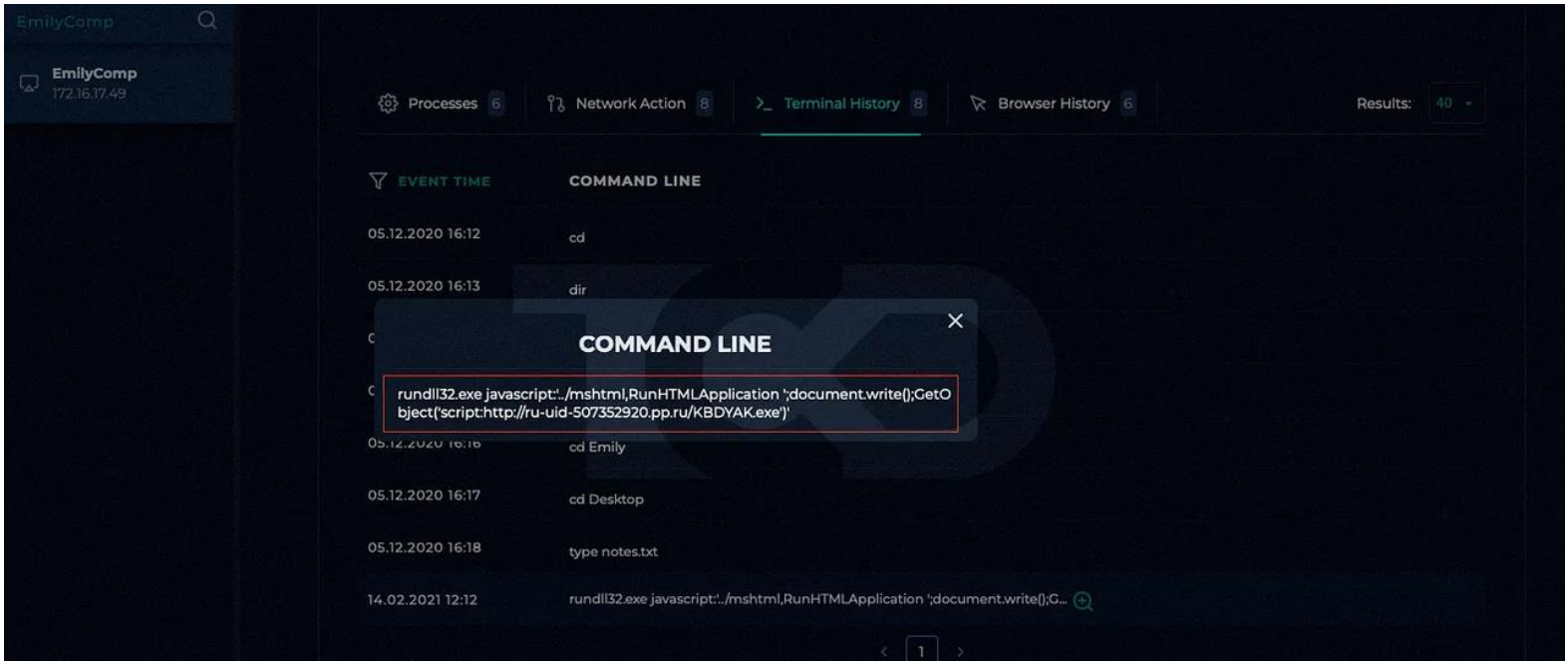
📤 Escalonamento:

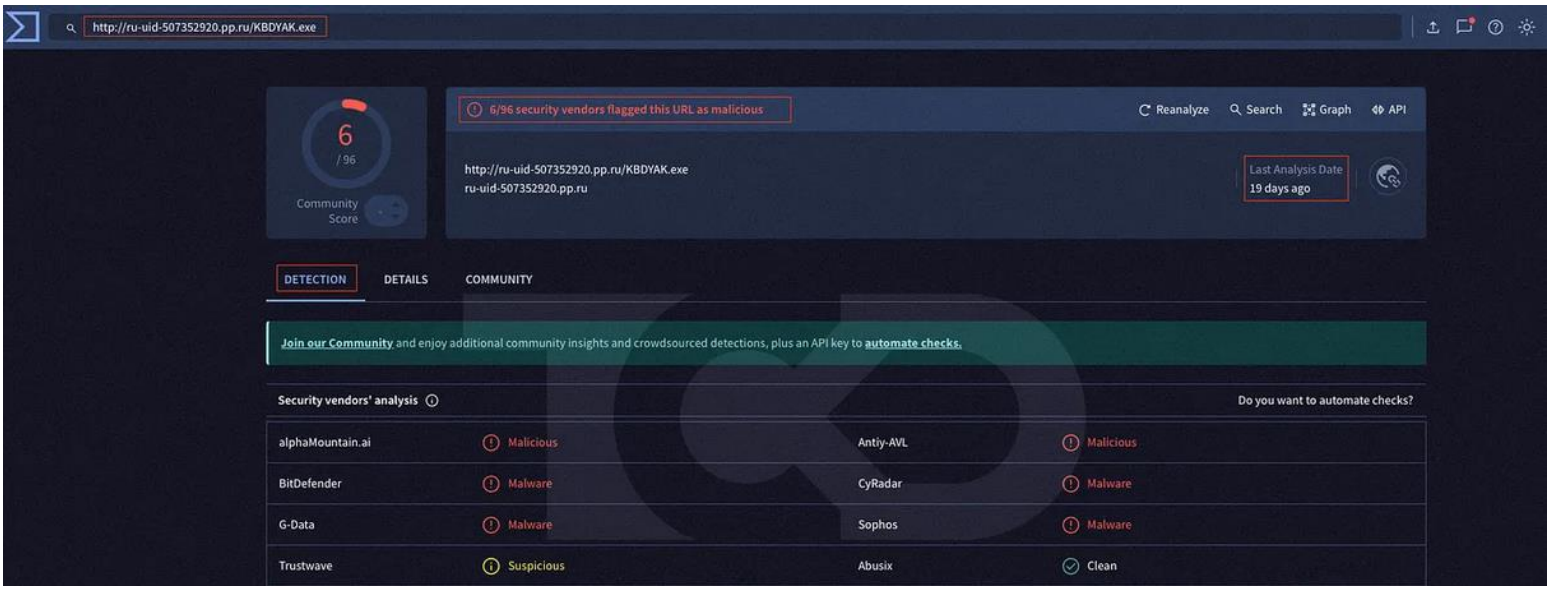
Todas as evidências foram encaminhadas para o time N2 para análise de persistência ou possíveis exfiltrações.

🖼️ Evidências / IOCs:

Tipo	Valor	Descrição
URL	hxxp://mogagrocol.ru	Domínio russo, origem do phishing
URL	hxxp://ru-uid-507352920.pp.ru/KBDYAK.exe	URL de malware (KBDYAK.exe)
IP externo	91.189.114[.]8	IP vinculado ao domínio malicioso
Host origem	172.16.17.49	Host da colaboradora Ellie
E-mail	ellie@letsdefend.io	E-mail utilizado na requisição






http://ru-uid-507352920.pp.ru/KBDYAK.exe
6
/ 96
Community Score
6/96 security vendors flagged this URL as malicious
Reanalyze
Search
Graph
API
http://ru-uid-507352920.pp.ru/KBDYAK.exe
ru-uid-507352920.pp.ru
Last Analysis Date
19 days ago
DETECTION
DETAILS
COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
alphaMountain.ai
Malicious
Antiy-AVL
Malicious
BitDefender
Malware
CyRadar
Malware
G-Data
Malware
Sophos
Malware
Trustwave
Suspicious
Abusix
Clean