
CRACK!
Hadoop
cluster node
HTTP request: pan.tenire[.]com
ELF
ALERT
ALERT!
REAL TIME ALERT:
DARKTRACE ALARMS
COMMAND
chmod 777
HTTP LOGS
chmod 777
MAS
شنو هاد Chaos؟!
تنبيه من Darktrace:
pan.tenire[.]com


السيرفرات كتقرصن!
PROXY-as-a-Service
SOCKS proxy!
HADOOP: misconfigured!
SSH
SSH
proxy
PROXY
PROXY
PROXY
PROXY proxy
MAS
BOOM!
RRIP!
ZZZT!
EXECUTION // FAILED SECURITY


Timeline
Timeline
Infrastructure
Silver Fox
Network
Honeypot
HTTP POST
pan.tenire[.]com
Silver Fox" network
pan.tenire[.]com
SOCKS module
SSH propagation functions
هاد ELF فيه SOCKS module
خاصنا traces ديال pan.tenire
SSSHK PING ECHOS.
DATA LOGS CRACEDLY TRASING EVIDENCE.
MAS
PING ECHOS.
SOCKS module


SYSTEM INTEGRITY: 100%
API LATENCY:
BACK TO NORMAL
BOTNET ISOLATED
BOTNET ISOLATED
درنا patch
وسدينا الثغرة
وقفناه!
Hecker
Patch applied:
cloud_vulnerabiiity/fix_01
SHING!
WHOOSH
WHOOSH
SOCKS
SOCKS
MAS
Firewall rules:
ACTIVE
(Malicious traffic filtered)
SECURE_STORAGE
SECURE_STORAGE
Isolated nodes:
42 (Noneypot redirection success)
rm -f /tmp/chaos_agent.sh
DELETE