LASTLINE PRESENTS

MALTOONS

NAME

LOKI AKA: PONY OR FAREIT

YEAR FIRST RELEASED	2015
ORIGINS	EASTERN EUROPE
PRIMARY OBJECTIVE	CREDENTIAL STEALER
SPECIFIC TARGETS	USERNAMES AND PASSWORDS
	monkey123 •••••••••
BEHAVIORS DISPLAYED	DELIVERED IN EMAIL VIA WEAPONISED MICROSOFT OFFICE FILES WITH THE ABILITY TO STEAL FROM MANY APPLICATIONS
ESTIMATED TOTAL NUMBER OF VARIATIONS	UNIQUE VARIANTS GENERATED EVERY DAY
ESTIMATED NUMBER OF SYSTEMS INFECTED	TENS OF THOUSANDS
STAND OUT FEATURE	REFERENCES DANTES INFERNO AND ENABLING THE SALE OF STOLEN ACCOUNTS ON DARK WEB MARKETS
DELIVERY METHOD	PRIMARLIY EMAIL AND RECENTLY SCRIPTLETS IN MICROSOFT OFFICE ATTACHMENTS
FILE TYPE	MICROSOFT OFFICE FILES USE POWERSHELL TO GET LOKI .EXE FILE
STRAIN (W/IN A FAMILY)	INFO-STEALER
TARGET VERTICALS	ALL
EVASION TECHNIQUES	CHECKS FOR ANALYSIS TOOLS, DISK SIZE, RUSSIAN KEYBOARD, SLEEP EVASIONS
IP ADDRESS THAT THEY TALK TO (WHERE BAD IP LIVES)	HAS "CKAV.RU" IN THE C2 CONTROL STRING
C&C - DEPENDENCE, TYPES OF CONTROLS, ETC	MANY C2 STRUCTURES IN PLACE; LOKI OPERATORS USE DISCREET INFRASTRUCTURE RESULTING IN NUMEROUS IP ADDRESSES GLOBALLY
SUGGESTED ERADICATION	LASTLINE ENTERPRISE

lastline™

CALL 877-671-3239 | WWW.LASTLINE.COM