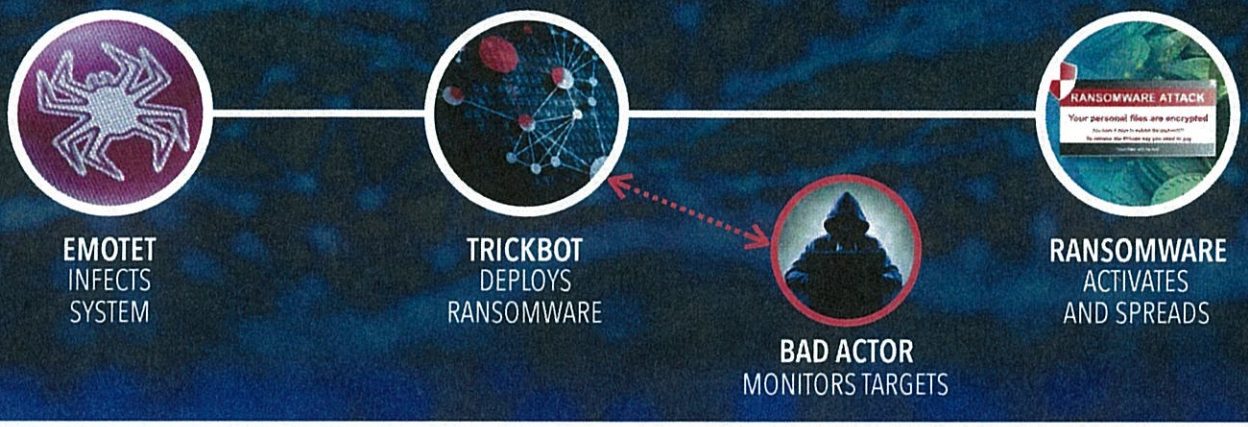
RIC one NEW YORK STATE REGIONAL INFORMATION CENTERS
DATA SECURITY **THREAT LANDSCAPE**

As cybersecurity vulnerabilities become more prevalent across the nation, this resource is designed to provide an overview of the current threat landscape and offers district leaders a reminder of important protections that should be implemented to help mitigate risks associated with recent cyber threats.

EMOTET INFILTRATES AND DEPLOYS ***TRICKBOT*** STEALS CREDENTIALS AND SPREADS ***RYUK RANSOMWARE***



SYSTEM PROTECTION REMINDERS

VULNERABILITY MANAGEMENT — **Patch known vulnerabilities on all systems, but in particular those systems that house sensitive data.**

SYSTEM BACKUPS — **Ensure backups for critical systems are in place and audit backups for completion and functionality.**

SYSTEM HARDENING — **Ensure anti-virus is installed and up-to-date, enable firewalls, close unnecessary ports, and disable non-essential services.**

IDENTITY MANAGEMENT — **Ensure accounts have appropriate permission levels. Domain Admin accounts should never be used to access workstations.**

APPLICATION SECURITY — **Only use district approved softwares, audit system access, and isolate critical infrastructure.**

Ensure ALL staff members are trained on Data Security best practices, particularly Email Phishing Recognition.

SYSTEM PATCHING TARGET TIMEFRAMES

TYPE OF UPDATE	COMPLETE WITHIN
SECURITY AND CRITICAL	1 to 3 WEEKS
HIGH PRIORITY	1 to 2 MONTHS
LOW PRIORITY	3 to 4 MONTHS