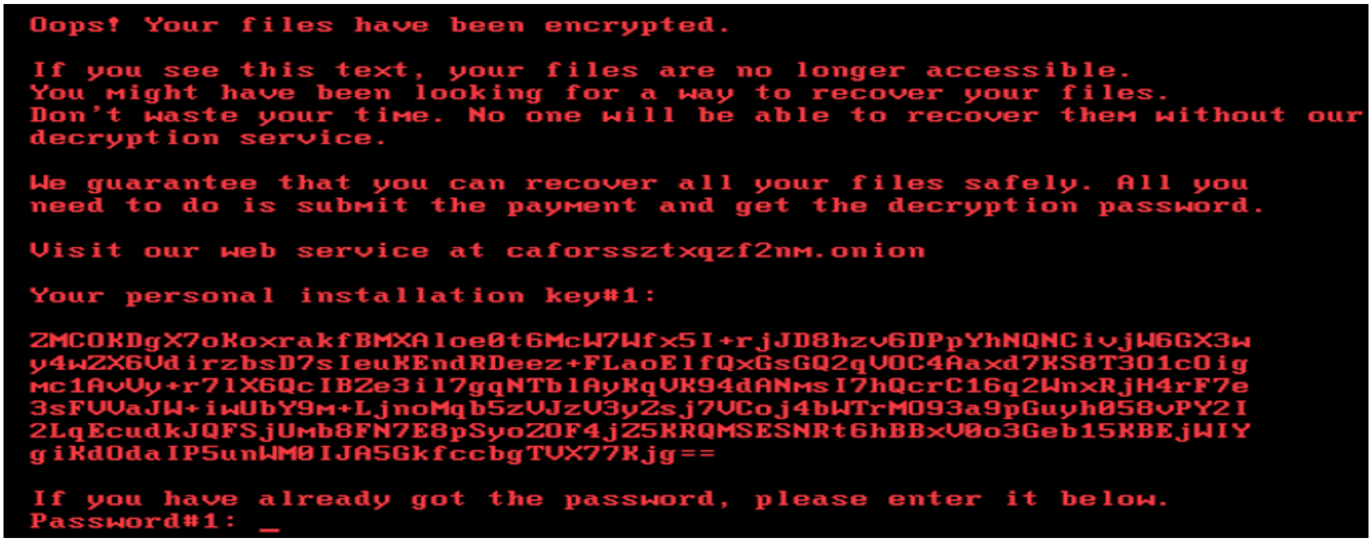
Case Study

Strengthening Security Posture across the organization

Large Public Employee Union

PROTECTING COMPANIES FROM RANSOMWARE ATTACKS



```
Oops! Your files have been encrypted.

If you see this text, your files are no longer accessible.
You might have been looking for a way to recover your files.
Don't waste your time. No one will be able to recover them without our
decryption service.

We guarantee that you can recover all your files safely. All you
need to do is submit the payment and get the decryption password.

Visit our web service at caforssztxqzf2nm.onion

Your personal installation key#1:

ZMCOKDgX7oKoxrakfBMXAloe0t6McW7Wfx5I+rjJD8hzv6DPpYhNQNCivjW6GX3w
y4wZX6VdirzbsD7sIeuKEndRDeez+FLaoElfQxGsGQ2qVOC4Aaxd7KS8T301cOig
mc1AvVy+r71X6QcIBZe3il7gqNTblAyKqVK94dANmsI7hQcrC16q2WnxRjH4rF7e
3sFVVaJW+iwUbY9m+LjnoMqb5zVJzV3yZsj7VCoj4bWTrM093a9pGuyh058vPY2I
2LqEcudkJQFSjUmb8FN7E8pSyoZ0F4jZ5KRQMSESNRt6hBBxV0o3Geb15KBEjWIY
giKd0daIP5unWM0IJA5GkfccbgTVX77Kjg==

If you have already got the password, please enter it below.
Password#1: _
```

CUSTOMER PROFILE

A large public employee Union with over 150,000 members, locations throughout the State.

CHALLENGES:

- ✓ Lack of visibility
- ✓ Out-of-date technologies
- ✓ Deficient Policies
- ✓ Manual Patch management

RESULTS:

- ✓ Deployment of Next Generation Solutions
- ✓Established Policies and Procedures
- ✓Incident Response Plan & Retainer
- ✓ Automated procedures

THE PROBLEM

The Union was compromised right before the holiday season, taking down their network and bringing business to a complete halt. Multiple endpoints, servers, strategic backups as well as the Active Directory Server were either compromised or it's data encrypted.

The Organization was struggling to get back on-line, while the employees were forced to revert to manual processes that were both slow and limited. Critical business processes and day to day operations were ceased and the organization was scrambling to recover.

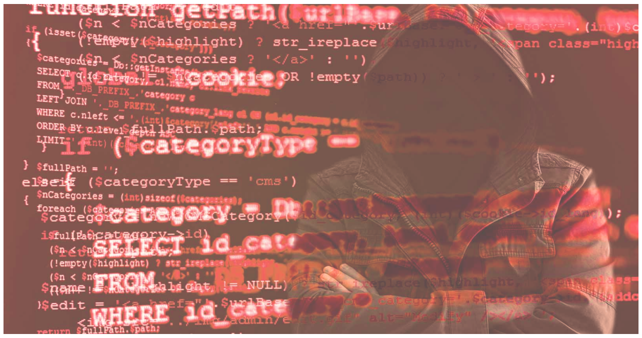
SCOPE & CRITERIA

The situation was grave at the time iPRESIDIUM was engaged with the client to conduct a forensic investigation. Within 1 hour, our team was on site and deploying agents to the network to prevent further spread and contain the attack.

The investigation included:

- All systems
- Perimeter security log output review
- Possible third-party breach
- Severity and nature of incident
- Analysis of internal response to incident
- The potential scope of compromise

iPRESIDIUM'S primary objective was to define the nature and scope of the compromise, assist in the tactical planning and remediation of any compromises found, and assist the organization to extend their capability to detect and respond to future incidents and/or suspicious activity strategically and effectively. iPRESIDIUM would attempt to determine if the attack was targeted and if any major threat actors were involved in the incident.



ENGAGEMENT

iPRESIDIUM Incident Response Team moved quickly to contain the threat, by deploying agents across the network infrastructure to prevent further damage. We quickly identified **thirteen** (13) compromised internal systems, **eighteen** (18) incidents of suspicious or malicious behavior and a defined overall scope of compromise of **High**.

iPRESIDIUM remediated the compromised systems immediately and continued to monitor for signs of attack for 30 days after the initial reported incident.

THE SOLUTION

The entire Incident Response engagement took 2 weeks to complete and the following recommendations were provided to the client:

- Expire all existing passwords.
- Establish complex passwords with 90-day expiration and 24-month reuse policy.
- Establish 2FA for administrators and (PCI-HIPAA, etc.,) sensitive users.
- Cloud backups for all mission critical data.
- Annual Pen Testing to ensure security measures are continued.
- Replace out-of-date Firewall
- Replace former endpoint technology with next generation Threat Hunting platform.

Following iPRESIDIUM'S Incident Response engagement, the client was able to quickly establish new security policies and procedures to strengthen their security posture. The organization established a newly formed cyber security committee to review policies and establish best practices. New security solutions were deployed;

- Firewall
- Endpoint
- Patch management

These next generation technologies were deployed replacing older, and in some instances, non-existent platforms. Security automation tools and processes are now deployed to mitigate risks and proactively secure the network. Newly established backup and restoration procedures are regularly tested. In addition, iPRESIDIUM was contracted as the Union's Incident Response IR approved by their Cyber Insurance carrier and currently on retainer.

About iPRESIDIUM

iPRESIDIUM is a cyber security and risk advisory firm. We provide end-to-end enterprise security services for private and public entities of all sizes. iPRESIDIUM helps customers protect their business, employees, data, and their reputations. We succeed by offering our clients cutting edge technologies with best-in-class security solutions, experienced industry professionals proficient in cyber security and managed service platforms. Our goal, to deliver our clients' the peace of mind they need so that they can focus on their business.

Since its inception in 2002, iPRESIDIUM has successfully exceeded the security needs of numerous organizations, across the following sectors: Healthcare, Retail, Education, Government and Public Sector, Financial, Technology, Hospitality, Insurance, Transportation and Manufacturing as well as over 50 US federal agencies and the intelligence communities.

iPRESIDIUM

www.ipresidium.com | info@ipresidium.com | 949-721-6612